UNIVERSIDADE FEDERAL DO MARANHÃO

Programa de Pós-Graduação em Ciência da Computação

Christiano Anderson Neitzke

Enhancing LGPD Compliance: A Specialized Checklist and Implementation Templates for Governmental Software Systems

São Luís - MA

2025

Christiano Anderson Neitzke

Enhancing LGPD Compliance: A Specialized Checklist and Implementation Templates for Governmental Software Systems

Thesis submitted as a partial requirement for the degree of Master of Science in Computer Science to the Graduate Program in Computer Science at the Federal University of Maranhão.

Graduate Program in Computer Science

Federal University of Maranhão

Supervisor: Prof. Dr. Davi Viana

Co-supervisor: Prof. Dr. Mario Teixeira

São Luís - MA

2025

Neitzke, Christiano Anderson.

Enhancing LGPD Compliance: A Specialized Checklist and Implementation Templates for Governmental Software Systems / Christiano Anderson Neitzke. - 2025.

142 f.

Coorientador: Mário Antonio Meireles Teixeira.
Orientador: Davi Viana dos Santos.
Dissertação (Mestrado) - Programa de Pós-graduação em Ciência da Computação/CCET, Universidade Federal do Maranhão, São Luís, 2025.

1. Inspection Checklist. 2. General Data Protection Law. 3. Lgpd. I. Santos, Davi Viana dos. II. Teixeira, Mario Antonio Meireles. III. Título.

Christiano Anderson Neitzke

Enhancing LGPD Compliance: A Specialized Checklist and Implementation Templates for Governmental Software Systems

Thesis submitted as a partial requirement for the degree of Master of Science in Computer Science to the Graduate Program in Computer Science at the Federal University of Maranhão.

Thesis defense on February 21, 2025, in São Luís - MA:

Prof. Dr. Davi Viana
Supervisor
Federal University of Maranhão

Prof. Dr. Mario Teixeira
Co-supervisor
Federal University of Maranhão

Prof. Dr. Luis Rivero
Internal Examiner
Federal University of Maranhão

Prof. Dr. Awdren Fontão
External Examiner
Federal University of Mato Grosso do Sul

São Luís - MA
2025

To my precious family, whose love and encouragement sustained me every step of the way.

Acknowledgements

The completion of this work would have been impossible without the support and understanding of several people who, directly or indirectly, contributed to the achievement of this very important stage of my academic life.

First of all, I am immensely grateful to my family and my beloved wife for their constant support, patience, and affection throughout the entire study journey. Your love and encouragement were fundamental to my continued progress, even in the face of the most difficult challenges.

To my advisors, Prof. Davi Viana and Prof. Mário Meireles, I express my deepest gratitude for their patience, valuable guidance, and trust in the development of this research. Your guidance was essential for maturing ideas and completing this work.

I also thank Prof. Luis Rivero, whose contributions always provided enriching perspectives and helped elevate the quality of this academic work. Your observations and suggestions were extremely relevant to the study's development.

A special thanks to Prof. Awdren Fontão for his significant contributions to this research, as an external examiner in my defense. His insightful observations and questions greatly enriched my academic and professional growth.

To my colleagues from TRE-MA and UFMA, who kindly dedicated their time to collaborate, question, and contribute to this research, I extend my sincere thanks. Your contributions helped shape and refine various parts of this work.

Finally, but no less importantly, I thank my friends Sebastião Penha, Amora Sukar, and Paulo Correa, who offered support and encouragement by my side. Your friendship and words of encouragement were a great foundation throughout this master's journey.

To all of you, my most sincere thank you!

"Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect."

(Bruce Schneier)

Resumo

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece diretrizes para o tratamento de dados pessoais. No entanto, compreender e implementar a LGPD apresenta desafios significativos para analistas de requisitos, particularmente na identificação e operacionalização de requisitos de privacidade. Esta dissertação adapta, avalia e aprimora o checklist LGPD-Check para uso em organizações públicas. O LGPD-Check é um método projetado para avaliar a conformidade de sistemas de software com os atributos de qualidade exigidos pela LGPD, abrangendo categorias como transparência de dados, consentimento do usuário, direitos do usuário, segurança de dados e responsabilidade do controlador. Aprimoramos o checklist incorporando requisitos específicos exigidos pelo Tribunal de Contas da União (TCU) e o aplicamos em uma organização governamental para avaliar sua eficácia. Nosso estudo envolveu oito profissionais de TI. Os resultados indicaram que o checklist apoia efetivamente a detecção de defeitos em sistemas de software e levou a melhorias do LGPD-Check. Além de atualizar itens e recomendações, desenvolvemos templates para auxiliar os inspetores no uso do checklist. Esses templates fornecem orientações sobre como tratar questões de não conformidade e implementar melhorias nos sistemas avaliados. Posteriormente, aplicamos o LGPD-Check a dois sistemas reais de uma instituição acadêmica federal, o que nos permitiu discutir os benefícios, desafios e refinamentos necessários relacionados às recomendações e templates. Nossas descobertas revelaram que 57,4% dos itens avaliados não atendiam aos padrões legais, indicando lacunas substanciais nos processos e práticas de proteção de dados. O feedback do grupo focal sugeriu que o checklist revisado e os templates auxiliam na identificação de problemas de conformidade de software com a LGPD. Apesar de algumas limitações, como a necessidade de mais estudos para generalizar os resultados e explorar aplicações em outros domínios, nosso trabalho contribui para aprimorar a conformidade com a LGPD em sistemas de software, particularmente no setor público.

Palavras-chave: inspection checklist, General Data Protection Law, LGPD.

Abstract

The Brazilian General Data Protection Law (LGPD) establishes guidelines for handling personal data. However, understanding and implementing the LGPD presents significant challenges for requirements analysts, particularly in identifying and operationalizing privacy requirements. This master's thesis adapts, evaluates, and enhances the LGPD-Check checklist for use in public organizations. LGPD-Check is a method designed to assess software systems' compliance with LGPD-mandated quality attributes, covering categories such as data transparency, user consent, user rights, data security, and controller responsibility. We improved the checklist by incorporating specific requirements demanded by the Federal Court of Accounts (TCU) and applied it within a government organization to assess its effectiveness. Our case study involved eight IT professionals. Results indicated that the checklist effectively supports the detection of defects in software systems and has led to significant enhancements of LGPD-Check. In addition to updating items and recommendations, we developed templates to assist inspectors in using the checklist. These templates provide guidance on addressing non-compliance issues and implementing improvements in the evaluated systems. Subsequently, we applied LGPD-Check to two real systems from a federal academic institution, which allowed us to discuss the benefits, challenges, and necessary refinements related to the recommendations and templates. Our findings revealed that 57.4% of the evaluated items did not meet legal standards, indicating substantial gaps in data protection processes and practices. Feedback from the focus group suggested that the revised checklist and templates help identify software compliance issues with the LGPD. Despite some limitations, such as the need for further studies to generalize the results and explore applications in other domains, our work contributes to enhancing LGPD compliance in software systems, particularly within the public sector.

Keywords: inspection checklist, General Data Protection Law, LGPD.

List of Figures

List of Tables

List of abbreviations and acronyms

AES	*Advanced Encryption Standard*
ANPD	*National Data Protection Authority*
DPIA	*Data Protection Impact Assessment*
DPO	*Data Protection Office*
DLT	*Distributed Ledger Technology*
GPPR	*General Data Protection Regulation*
IAM	*Identity and Access Management*
IFES	*Federal Higher Education Institutions*
LGPD	*General Data Protection Law*
MFA	*Multifactor Authentication*
PbD	*Privacy by Design*
RBAC	*Role-Based Access Control*
RLS	*Row Level Security*
SHA	*Secure Hash Algorithm*
SSL	*Secure Sockets Layer*
TAM	*Technology Acceptance Model*
TCLE	*Free and Informed Consent Form*
TCU	*Federal Court of Auditors*
TDE	*Transparent Data Encryption*
TLS	*Transport Layer Security*
TRE-MA	*Electoral Regional Court of Maranhão*
UFMA	*Federal University of Maranhão*
UFMS	*Federal University of Mato Grosso do Sul*

Contents

1 Introduction

This chapter introduces this master's thesis by contextualizing and outlining the objectives, motivation, and research methodology. Additionally, the structure and organization of this document are detailed.

1.1 Contextualization

With the widespread adoption of mobile devices and social networks, the massive production of data has made privacy and personal data protection global concerns and essential needs. In 2016, the European Union enacted the General Data Protection Regulation (GDPR), Regulation 2016/679, in response to technological advancements. This legal framework governs privacy and data protection by setting comprehensive guidelines for processing personal data across the European continent (European Commission, 2016). It also establishes a unified and consistent regulatory standard within the European Union, ensuring legal coherence and promoting data protection best practices (RINGMANN; LANGWEG; WALDVOGEL, 2018).

The implementation of the GDPR in Europe has motivated countries like Brazil to develop their data protection regulations, culminating in the creation of the General Data Protection Law (*Lei Geral de Proteção de Dados Pessoais* - LGPD) - Law 13.709/2018. This legal framework introduces critical provisions on privacy and data protection for Brazilian society (BRASIL, 2018). Both regulatory systems, GDPR and LGPD, aim to strengthen security and foster trust in the relationship between users and organizations (LORENZON, 2021).

LGPD is based on principles such as respect for privacy, consumer defense, inviolability of intimacy, and especially, the protection of human rights (BRASIL, 2018). The primary purpose of the law is to promote responsible and fair processing of personal data by companies, in addition to safeguarding users' right to privacy in an increasingly connected and data-driven global scenario (DUARTE et al., 2020). Organizations must be capable of complying with all guidelines outlined in the data protection law, and non-compliance exposes companies to administrative sanctions, potentially leading to financial penalties (SOUZA et al., 2020). In addition to these punishments, non-compliance with the law can lead to several societal problems, such as user data leaks, violation of consumer rights, and prohibition of personal data collection and processing, among others (MACHADO et al., 2019). Therefore, companies must concern themselves with how they integrate data protection into the culture of their organizational practices, proposing new rules for compliance with the law, establishing a privacy and security policy, informative actions for their employees, and other aspects related to adherence to the LGPD (PELOSO et al., 2019).

Many organizations are not prepared to comply with Brazilian legislation, as their software engineers have demonstrated little knowledge of the law (PELOSO et al., 2019). The study conducted by Ferrão et al. (2021) supports this observation through a survey involving Brazilian organizations from both the public and private sectors. The survey assessed compliance with the LGPD based on the perceptions of 105 information technology professionals employed in these organizations. Approximately 16.3% of organizations have not implemented a procedure to ensure compliance with the principles of the LGPD. Furthermore, 20% of organizations lack a communication process to inform personal data holders about potential data breaches. Additionally, only 27% of organizations process publicly accessible personal data in accordance with the principles of good faith and the guidelines established by the LGPD.

Canedo et al. (2021) investigated the perceptions of members of agile software development teams from various organizations concerning the impact of the LGPD on software development process activities. The results reveal that agile teams are familiar with data privacy legislation concepts but do not employ the techniques proposed in the literature for eliciting privacy requirements. Additionally, agile teams encounter problems with outdated software requirements specifications and a lack of stakeholder knowledge regarding data privacy. Therefore, further investigation is necessary to determine how to support software engineers in applying the law and the impact of such applications on businesses.

In 2022, the Federal Court of Auditors (TCU) published a Diagnostic Report on the Degree of Implementation of the LGPD in the Federal Public Administration. This audit assessed 382 federal public agencies in Brazil. It showed that most institutions are in the early stages of implementing the LGPD and recommending initiatives to be adopted by federal public agencies (Tribunal de Contas da União, 2022). According to the TCU's research, the implementation levels among the audited organizations were distributed as follows: 17.8% are at the inexpressive level, 58.9% are at the initial level, 20.4% are at the intermediate level, and 2.9% are at the advanced level.

In this context, developing tools that assist organizations and individuals in creating software that is compliant with the LGPD is essential to address global demands for privacy and personal data protection. Achieving this goal requires artifacts, tools, and methodologies that structure legal knowledge and support professionals in identifying, understanding, and operationalizing requirements established in legal frameworks such as the LGPD (SHAPIRO, 2010).

1.2 Problem and Justification

Achieving compliance with the Brazilian General Data Protection Law presents a complex challenge for organizations due to its dual legal and technical requirements. The need for adaptation extends beyond implementing technological solutions, encompassing organizational policies, management practices, and cultural changes. Recent studies indicate that many organizations remain unprepared to comply with the LGPD due to inadequate knowledge about the legislation and its operational implications (FERRÃO et al., 2021; CANEDO et al., 2021).

Furthermore, many Brazilian public institutions face challenges in implementing the LGPD due to a lack of technical and human resources. Official reports, such as the one published by Tribunal de Contas da União (2022), reveal that many federal public agencies are still in the initial stages of LGPD compliance implementation. The TCU audit also indicates that only 29% of organizations have a Training Plan that encompasses personal data protection, representing a significant organizational risk. Moreover, only 16% of organizations have implemented access control across all systems that process personal data, exposing themselves to a high risk of unauthorized access to this data and, consequently, to the violation of citizens' privacy (Tribunal de Contas da União, 2022).

Another recurring issue in many institutions, especially public ones, is using legacy systems that do not support LGPD requirements, such as consent records and audits. This is compounded by the shortage of trained data protection professionals and the lack of budget to invest in technologies, training, and specialized consultancies that could assist in LGPD compliance.

Given this context, this research's central problem is: **"How can we support software development teams to enhance system compliance with the LGPD in public agencies?"**

Thus, this research is justified by its contribution to improving privacy and personal data protection in an increasingly digital society, where handling improper information can compromise fundamental rights such as privacy and security.

1.3 Objectives

Given the presented context, this research's primary objective is **to develop artifacts that support software development teams in improving system compliance with the LGPD in public institutions**. To achieve this, the evolution of an inspection checklist, enhanced for public administration, not only enables the early detection of issues, thereby avoiding rework and waste, but also facilitates the efficient correction of non-conformities. Furthermore, providing templates and recommendations linked to the checklist items directly contributes to resolving identified defects.

To achieve this goal, the following specific objectives were established:

- **Enhance an existing checklist**, incorporating items required by regulatory bodies within the context of public institutions, considering legal guidelines and best practices;
- **Evaluate the checklist's feasibility** in a public agency environment by investigating its applicability and acceptability within the institution's technical context;
- **Develop a set of templates and recommendations** designed to support the correction of non-conformities identified by the checklist, promoting a systematic approach for implementing improvements;
- **Evaluate the developed tools** by conducting a case study, identifying improvement opportunities based on results obtained from their practical application in the industry.

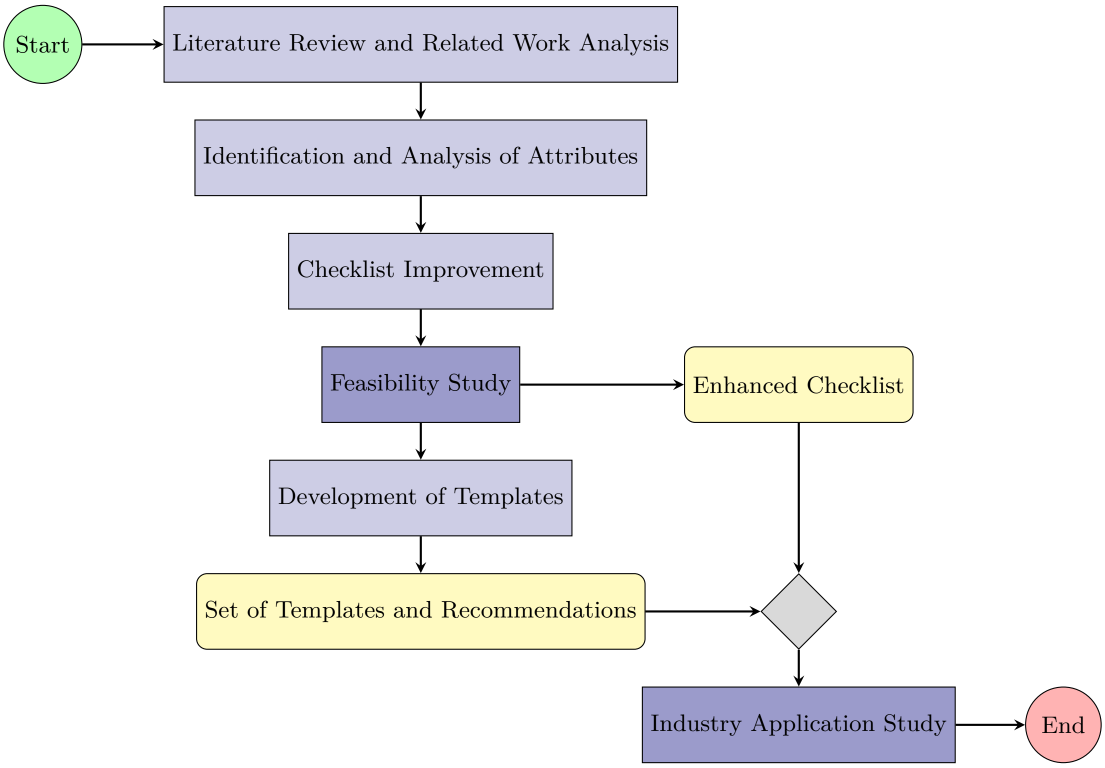
This approach aims to contribute to enhancing system compliance with the LGPD, fostering safer data processing practices within Brazilian public institutions.

1.4 Methodology

The development of this study follows a methodology based on adaptations of works by Ringmann, Langweg e Waldvogel (2018), which focuses on data protection, and Kalinowski, Spínola e Travassos (2004), which addresses experimentation in software engineering. This approach encompasses a literature review and exploratory studies to refine an initial proposal for a software inspection checklist, initially proposed by Mendes, Viana e Rivero (2021), aiming to specialize and apply it in public agencies. The methodology will be elaborated in the subsequent sections and is visually represented in Figure 1.

- **Literature Review and Related Work Analysis:** Given that the LGPD is a relatively recent regulation with limited academic production, it becomes essential to investigate the state of the art in Brazil, identifying research gaps and relevant contributions. Additionally, it is necessary to explore the literature on privacy and personal data protection to identify best practices and inherent challenges in implementing these concepts in software engineering.

Figure 1 – Methodology Overview


Start
Literature Review and Related Work Analysis
Identification and Analysis of Attributes
Checklist Improvement
Feasibility Study
Enhanced Checklist
Development of Templates
Set of Templates and Recommendations
Industry Application Study
End

- **Identification and Analysis of Attributes:** A study and analysis of the initial version of the checklist proposed by Mendes, Viana e Rivero (2021) and the audit conducted by Tribunal de Contas da União (2022) is carried out. This stage aims to identify and extract new quality attributes from the audit and incorporate them into an enhanced checklist version.

- **Checklist Improvement:** Based on the identified attributes, new items are added to the initial version developed by Mendes, Viana e Rivero (2021) to expand its scope and precision. This stage seeks to align the checklist with the evaluative practices the TCU employs, strengthening its applicability in the context of federal public institutions.

- **Feasibility Study:** To validate the proposal from a practical perspective, a proof of concept is performed by applying the checklist in a public agency. This application allows non-compliance identification in departmental systems, verifying the instrument's effectiveness in detecting data protection-related issues.

- **Checklist Evolution:** Based on the feasibility study results, the checklist is enhanced by incorporating improvement recommendations, correcting identified errors, and considering suggestions provided by the involved teams. Additionally, specific templates and recommendations for each checklist item are developed, facilitating its application and supporting development teams in resolving detected non-compliance.

- **Industry Application of Templates:** A case study evaluates the practical application of templates and recommendations in an industrial context. This stage aims to gather additional relevant information for the continuous improvement of the checklist, resulting in a new iteration of the more robust instrument tailored to the public sector's needs.

1.5 Document Organization

This thesis is organized into five main chapters, in addition to Chapter 1, which presents the research context, problem statement, justification, objectives, and methodology. The organization of the subsequent chapters is described as follows:

Chapter 2 addresses the theoretical foundation, exploring concepts related to privacy and personal data protection in software engineering. It presents key terms and definitions associated with the Brazilian General Data Protection Law and relevant aspects of software inspection applicable to this research.

Chapter 3 provides a detailed description of the refinement process for the LGPD-Check checklist. It discusses the steps performed during its development, including a feasibility study conducted in a public sector organization. This study highlights the checklist's practical application and evaluates its effectiveness through qualitative analysis.

Chapter 4 presents the proposed improvements for a new version of the LGPD-Check, emphasizing the development of templates and specific recommendations for each checklist item, aiming to support the mitigation of identified non-conformities. The chapter also reports a case study involving real systems from a Federal University, detailing the practical application of the templates and the evaluations conducted. Additionally, it discusses the qualitative results obtained, including relevant findings from a focus group session.

Finally, Chapter 5 presents the concluding remarks of this research, highlighting its main contributions to the field of data protection, its limitations, potential threats, and possible directions for future studies.

2 Background and Related Work

This chapter provides a concise conceptual overview of the principles of Privacy and Data Protection, the General Data Protection Law, and the fundamental aspects of Software Inspection. Its objective is to establish a theoretical foundation by exploring relevant concepts, legal frameworks, and technical methodologies, offering essential context for understanding the research's scope and practical applications.

2.1 Privacy and Data Protection

When exploring the privacy and data protection literature, the widely recognized concept of Privacy by Design (PbD) stands out. According to Cavoukian et al. (2021), this approach constitutes a methodology aimed at ensuring privacy protection from the very inception of any information technology system or business practice involving individuals and their fundamental freedoms.

Seven fundamental principles are defined and applied in the practice of PbD, emphasizing that this approach should permeate all aspects of technology, processes, organizational culture, and corporate governance within companies and institutions (CAVOUKIAN et al., 2021):

1. **Proactive, Not Reactive; Preventive, Not Corrective:** The PbD approach adopts preventive and proactive measures, anticipating and avoiding privacy breaches before they occur. This involves identifying and addressing potential failures during the planning phase, prior to product or service development and launch.

2. **Privacy by Default:** This principle ensures the highest level of privacy protection by default, regardless of user action. Personal data is automatically protected, ensuring privacy remains intact even if the individual takes no specific measures.

3. **Privacy Embedded into Design:** Privacy must be comprehensively integrated into technologies and business practices, making it an essential and inherent component of the system, rather than an optional add-on.

4. **Full Functionality – Positive-Sum, Not Zero-Sum:** This principle seeks to balance all legitimate interests, promoting mutual benefits for individuals and society. It avoids a zero-sum approach, where privacy is viewed as an obstacle to technological progress.

5. **End-to-End Security and Lifecycle Data Protection:** Protection must be ensured from the initial data collection to its final destruction. Systems must guarantee the confidentiality, integrity, and availability of personal data throughout its entire lifecycle, minimizing risks and preventing abuses.

6. **Visibility and Transparency:** Privacy-related operations must be transparent and verifiable, ensuring that processes follow declared policies. Adequate documentation, public policy disclosure, and accessible communication channels are organizational measures that promote this principle.

7. **Respect for User Privacy – Focus on the Individual:** User interests and rights must be at the core of decision-making. This includes providing robust privacy standards, clear communication, and easy-to-use controls. Organizations must empower data subjects to manage their personal information actively, preventing misuse and abuse.

Data protection legislations adopted in Europe, represented by the General Data Protection Regulation, and in Brazil, by the General Data Protection Law, explicitly incorporate the concepts of Privacy by Design and Privacy by Default as methodological pillars to ensure privacy and data protection. In the context of the LGPD, these concepts are formally established in Article 46, §§ 1 and 2, reinforcing their application as guiding principles in the processing of personal data (BRASIL, 2018).

> Article 46. Data processing agents must adopt appropriate security measures, both technical and administrative, to protect personal data from unauthorized access, as well as accidental or unlawful incidents of destruction, loss, alteration, disclosure, or any form of improper or illegal processing.
>
> § 1. The national authority may establish minimum technical standards to implement the provisions of this article, taking into account the nature of the processed information, the specific characteristics of the processing activities, and the current state of technology, especially in the case of sensitive personal data, as well as the principles outlined in Article 6 of this Law.
>
> § 2. The measures referred to in the main section of this article **must be observed from the product or service design phase** through its execution.

Gürses, Troncoso e Diaz (2015) highlight the need for a paradigm shift among professionals responsible for the design and implementation of systems. The authors draw attention to common data collection and processing practices in software systems, where many professionals tend to gather as much data as possible without critically distinguishing between "data I can collect" and "data I need to collect" to meet the system's or functionality's specific purposes. This approach, often adopted automatically, can compromise privacy and compliance with data protection regulations (GÜRSES; TRONCOSO; DIAZ, 2015).

2.2 Brazilian General Data Protection Law

The LGPD came into effect in 2020, aligning with the European Union's GDPR. This regulatory convergence strengthens commercial and institutional relations between Brazil and the European Union by ensuring equivalent personal data protection standards. The LGPD establishes the foundation of Brazil's regulatory framework for data protection, serving as a legal milestone for personal information management practices (BRASIL, 2018).

The legislation clearly defines the boundaries for collecting, processing, storing, and sharing personal data, imposing administrative sanctions on organizations that violate its provisions. The LGPD regulates these operations across both the public and private sectors, promoting a comprehensive and balanced approach to personal data management in compliance with fundamental security and privacy principles (BRASIL, 2018).

The LGPD comprises 65 articles covering definitions, concepts, principles, sanctions, and requirements applicable to the processing of personal data (BRASIL, 2018). Among the key concepts outlined in the legislation are:

- **Personal Data:** Information related to an identified or identifiable natural person, such as name, identification number, address, or any data enabling direct or indirect identification of the individual.

- **Sensitive Personal Data:** Personal information revealing racial or ethnic origin, religious beliefs, health conditions, sexual orientation, political opinions, or genetic or biometric data associated with a specific person.

- **Anonymized Data:** Data that, after processing, cannot be linked to a specific individual, rendering the person non-identifiable.

- **Pseudonymization:** A data processing technique that reduces the likelihood of direct or indirect association of data with an individual, enabling re-identification through specific keys.

- **National Authority:** The regulatory body responsible for overseeing, implementing, and enforcing the LGPD throughout the national territory.

- **Data Subject:** The natural person to whom the personal data being processed relates.

- **Controller:** A natural or legal person, public or private, responsible for decisions related to personal data processing.
- **Processor:** A natural or legal person, public or private, that processes personal data on behalf of the controller, following its instructions.
- **Data Protection Officer (DPO):** The individual designated by the controller to act as a liaison between the controller, data subjects, and the National Data Protection Authority (ANPD).
- **Processing:** Any operation performed on personal data, including collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation, control, communication, transfer, dissemination, or extraction.

The principles established by the legislation constitute the fundamental basis for any personal data processing activity. These activities must be carried out in accordance with these ten principles, always respecting the duty of good faith (BRASIL, 2018). The principles are as follows:

1. **Purpose:** Personal data processing must occur for legitimate, specific, explicit purposes that are informed to the data subject, respecting the original purposes for which the data was collected.
2. **Adequacy:** The processing of personal data must be compatible with the purposes previously informed to the data subject, considering the context and nature of the processing performed.
3. **Necessity:** Personal data processing must be limited to what is strictly necessary to achieve the informed purposes, including only relevant, proportional, and non-excessive information.
4. **Free Access:** Data subjects have the right to access information about the processing of their data, including its form, duration, and entirety, in a facilitated and free manner.
5. **Data Quality:** Personal data must be accurate, clear, relevant, and up-to-date as needed to fulfill the purposes of processing.
6. **Transparency:** Data subjects must receive clear, precise, and easily accessible information about the processing of their data and the involved agents, considering potential commercial and industrial secrets.

7. **Security:** Appropriate technical and administrative measures must be adopted to protect personal data against unauthorized access and accidental or unlawful incidents, such as destruction, loss, alteration, communication, or improper dissemination.

8. **Prevention:** Preventive measures must be implemented to minimize potential damages resulting from personal data processing.

9. **Non-Discrimination:** The use of personal data for unlawful or abusive discriminatory practices is prohibited.

10. **Accountability and Accountability Reporting:** Data processing agents must demonstrate the adoption of effective measures to ensure compliance with personal data protection standards, proving the effectiveness of these actions.

Organizations face the challenge of ensuring the legal compliance of software systems as they strive to avoid administrative sanctions imposed by the ANPD. The penalties established by the LGPD range from warnings to financial sanctions, which may reach up to 2% of the company's annual revenue, capped at a maximum amount of R$ 50 million per violation (BRASIL, 2018).

2.3 Software Inspection

Software inspection involves visually reviewing a product to detect and identify anomalies, errors, and deviations from established standards and specifications (IEEE, 2008). This process primarily aims to improve the quality of software products, offering a cost-effective approach that significantly reduces rework (FAGAN, 1976). Regarding the process of software development and quality, inspection has proven to be a low-cost approach (KALINOWSKI; SPÍNOLA; TRAVASSOS, 2004), which possesses a rigorous and well-defined process that improves software quality, demonstrating an efficient technique in defect detection, thus reducing rework.

Mello, Massollar e Travassos (2011) highlights that selecting the appropriate inspection technique plays a critical role in the planning and outcomes of software product and project inspections. One commonly used technique is Ad-hoc inspection, which relies on the inspector's prior knowledge and is typically performed in an unstructured manner (SHULL et al., 1999), making it suitable for various types of artifacts.

Another widely adopted approach includes checklist-based inspection techniques, which utilize predefined questions, usually in a "Yes/No" format. These questions guide and support the inspector throughout the document review process, helping to identify potential issues (LAITENBERGER; EMAM; HARBICH, 2001).

In this context, Mendes, Viana e Rivero (2021) proposed an initial version of an inspection checklist designed to assess the compliance of software systems with Brazil's LGPD. This checklist drew from the law itself and a systematic literature mapping that included articles on assessment techniques and LGPD-related quality attributes. The checklist focused on the LGPD's quality attributes, meaning the characteristics and requirements established by the law to ensure system compliance and prevent legal and financial penalties. Additionally, it incorporated findings from a systematic literature mapping covering evaluation techniques and aspects related to the LGPD.

Later, the study was expanded by Neto et al. (2024), who proposed additions to the original checklist to support the verification of Internet of Things (IoT) based systems. They evaluated it in a private institution focused on industrial innovation, whose profile aligns with the target audience of the suggested mechanism. The evaluation was conducted through a case study, in which a post-inspection questionnaire was administered using the proposed checklist. Furthermore, the authors conducted a focus group to discuss the benefits, critical points, and potential improvements applicable to the checklist. The study yielded positive contributions regarding the use of the mechanism and the identification of security defects in the evaluated systems.

2.4 Related Works

In the course of investigating inspection techniques aligned with the principles of the Brazilian LGPD, even through initial exploratory methods, a growing interest from the Software Engineering community in the LGPD has become evident. Canedo et al. (2020) conducted a systematic literature review aimed at identifying research related to software privacy, privacy requirements, and the methodologies and techniques employed in their specification. The findings of this review revealed a significant knowledge deficit among information technology professionals concerning software privacy, legal requirements, and the guidelines stipulated by the LGPD.

Corroborating these findings, Peixoto et al. (2020) emphasize that many developers possess only an empirical understanding of privacy, as evidenced by their difficulty in correctly interpreting privacy requirements and their lack of familiarity with the legal provisions of the LGPD. These results underscore the need for continuous training and capacity-building to ensure that technology professionals are equipped to develop systems in compliance with current legislation.

In the context of GDPR, Becker et al. (2019) developed a software tool named Daisy aimed at enabling research institutions within the field of biomedicine to meet the accountability requirement. Upon analyzing storage and documentation, they found that the Daisy tool effectively fulfills the accountability requirement. Documentation presents itself as a significant challenge imposed by the GDPR and other laws, requiring the use of specific and dedicated tools for this context.

In the study conducted by Barati et al. (2021), a new technique was proposed for auditing and verifying operations performed on cloud computing user data. The research leverages blockchain network technologies to verify operations performed on user data transparently. To validate the feasibility of the proposed technique, the researchers used a health service as a case study. Although the study was based on a single scenario, the proposed architecture can be generalized to other situations.

In turn, Kubicek et al. (2022) developed a procedure to verify the GDPR consent compliance of marketing email-oriented websites. They evaluated 1,000 websites and 5,000 emails resulting from registrations on these sites. The study results suggest that many sites may violate European privacy regarding marketing emails. Non-compliance with these rules is typical, as it is complex to detect such violations concerning the holder's consent, especially when marketing for commercial companies.

Regarding the Brazilian Data Protection Law, the paper developed by Celidonio, Neves e Doná (2020) shows an enumeration of requirements mapped from the LGPD, considering the scenario of a financial organization. The authors present a diagnosis and the essential actions to adapt a corporation to the demands of the LGPD. However, it is noticeable that the described requirements lack adequate detailing that would favor a more fruitful consultation.

Additionally, Morte et al. (2020) propose an analysis of the technical characteristics related to using Distributed Ledger Technology (DLT) to treat personal data. The research concluded that DLT can be effectively employed, offering recommendations for treating personal data in compliance with the legislation stipulates.

Within the scope of evaluations, the work of Rojas (2020) analyzes an educational institution, through interviews with professionals working in this entity, based on a questionnaire. However, this tool includes only 13 questions in general, thereby limiting the meticulous examination of all aspects of the LGPD in the broad adaptation of software systems.

In another study, Araujo et al. (2021) introduced the LGPD4BP method for business processes. This method was implemented in a case study at the Federal University of Pernambuco and validated by a postgraduate group, which applied the approach and responded to a questionnaire about the ease and completeness of the proposal. The results of the evaluations carried out by the students revealed that the most challenging step is modeling the business process, not the components of the proposed method.

Canedo et al. (2022) have recently expanded their research into how companies respond to the LGPD, particularly in software development. This exploration pays special attention to the viewpoints of agile development teams two years post the LGPD's enactment. In addition to conducting a systematic literature review, in which 36 primary studies were picked, Canedo et al. (2022) also surveyed IT specialists and conducted semi-structured interviews. The results show that since the LGPD came into effect, Brazilian agile teams and companies have grown more cautious about privacy issues concerning user data. Despite this, agile teams are not fully utilizing available tools designed to aid in privacy requirement gathering.

Camêlo e Alves (2023) developed G-PRIV: a guide for specifying privacy requirements in compliance with the LGPD. The study helps requirements analysts define privacy requirements to ensure legal compliance. To achieve this goal, the researcher conducted exploratory interviews to investigate analysts' perspectives and highlight the challenges faced in specifying privacy requirements.

In 2024, Cerqueira (2024) created artifacts for inspecting privacy and personal data protection in software under the principles of the LGPD. The study focuses on designing artifacts that make the concepts and definitions from the first chapter of the law more tangible. Also, in 2024, Almeida (2024) proposed a structured process for assessing compliance with the LGPD in Federal Higher Education Institutions (IFES). The researcher designed a macro-process to help institutional managers adapt to the LGPD. The motivation for this project lies in tailoring the framework proposed by the Digital Government Secretariat to the specificities and culture of IFES.

Given the above, the urgency of seeking the best technological aspects is understood to assist professionals and companies in considering which strategy to follow to ensure compliance with data protection laws. However, the lack of adequate and widely disseminated studies for the academic and professional community still presents a challenge for software development teams, who need to implement the newly defined guidelines (CANEDO et al., 2021; FERRÃO et al., 2021; CANEDO et al., 2022). This work is motivated by the need to provide a viable and user-friendly technology that can be applied in real-world contexts by software engineers who wish to assess the compliance of their computational systems with the regulations.

2.5 Final Considerations

This chapter provided an overview of the fundamental concepts related to privacy and personal data protection, focusing on the understanding required for compliance with current legislation. Essential concepts such as definitions, principles, sanctions, and requirements established by the LGPD were discussed, emphasizing its role as a regulatory framework for data protection in Brazil.

Additionally, relevant aspects of software inspection and its contribution to ensuring

LGPD compliance were addressed. The integration of inspection practices allows for the identification of potential non-conformities in software systems, aiding in the detection and correction of security and privacy issues from the early stages of development.

In summary, the content presented in this chapter provided a conceptual foundation for the subsequent chapters of this thesis. Understanding the fundamentals of data protection and software inspection is essential for proposing a compliance verification framework for the LGPD, contributing to the advancement of privacy and personal data protection practices.

3 Enhancing LPGD-Check

This chapter delineates the critical phases executed during the refinement process of the LGPD-Check inspection technique. It presents the initial iteration of LGPD-Check and elucidates the methodological enhancements and modifications implemented throughout its developmental trajectory. Furthermore, it presents a feasibility study conducted within a public-sector organization, highlighting the proposed approach's practical application and evaluation.

3.1 Preliminary Version of the Checklist

The work by Mendes, Viana e Rivero (2021) introduced a preliminary version of an inspection checklist to assess software systems' compliance with the LGPD. This checklist was created by analyzing attributes extracted directly from the LGPD, complemented by systematic mapping of the existing literature and an additional informal review.

Regarding the search strategy, the following search string was applied to the digital libraries of ACM, IEEE, and SCOPUS:

```
((((“Technique" OR "Approach" OR "Model" OR "Method" OR "Framework" OR "Instrument") AND
("Evaluation" OR "Assessment" OR "Testing" OR "Measurement" OR "Tracking" OR "Recognition" OR
"Inspection")) OR ("Attribute" OR "Requirement" OR "Principle" OR "Feature" OR "Characteristic"
OR "Restriction")) AND ("LGPD" OR "RGPD" OR "GDPR" OR "GDPL" OR "General data protection law" OR
"General data protection regulation"))
```

This comprehensive search yielded a total of 961 articles. Following the rigorous application of all inclusion and exclusion criteria, 36 articles were ultimately selected for analysis. Of these, 35 articles presented quality attributes related to the GDPR, while only one article specifically addressed attributes of the LGPD (MENDES; VIANA; RIVERO, 2021).

In aggregate, combining the results of the systematic mapping with an informal search conducted through Google Scholar, a total of 44 articles were identified that reported quality attributes in the context of either LGPD or GDPR. This comprehensive approach ensured a thorough coverage of the relevant literature in the field of data protection regulation compliance (MENDES; VIANA; RIVERO, 2021).

The development of the proposed checklist adhered to the methodological recommendations outlined by Ringmann, Langweg e Waldvogel (2018) for the extraction and transformation of requirements and quality attributes into checklist items. This rigorous approach involved a systematic process of requirement elicitation and attribute identification from both academic literature and legal texts. Translating legal requirements into actionable technical specifications is critical in bridging the gap between regulatory compliance and practical implementation in software systems.

Mendes, Viana e Rivero (2021) categorized the checklist items into mandatory and non-mandatory components. The mandatory items are explicitly described in the Brazilian LGPD (BRASIL, 2018), and adherence to these provisions is essential for organizations, as this regulatory framework requires their compliance. Conversely, non-mandatory items are not stipulated in the LGPD but are highly recommended or optional, offering companies opportunities to improve their systems' compliance. These items are also derived from and described in other regulations, such as the GDPR (European Commission, 2016).

3.2 Enhancing the Inspection Checklist

The previously presented instrument was designed to assess any system based on the principles of the LGPD. However, in more specific cases, a more detailed analysis is required to identify potential issues. In this context, the section of the law that addresses good security practices outlines the responsibilities of the data controller, who must implement protective measures to safeguard personal data. This aspect is particularly important for public agencies, as they typically manage a vast amount of personal information, often of a sensitive nature. Given their role in providing essential services to citizens, any failure in data protection could lead to serious consequences, such as privacy violations and loss of public trust.

Based on these considerations, we have refined the checklist proposed by Mendes, Viana e Rivero (2021), resulting in an improved version. This updated checklist is primarily targeted at projects implemented within the context of public agencies and governmental institutions.

To enhance this inspection technique, we incorporated elements from the Diagnostic Report on the Degree of LGPD Implementation in the Federal Public Administration, a comprehensive audit conducted by Tribunal de Contas da União (2022). This extensive evaluation encompassed 382 federal public agencies in Brazil. The resulting report not only revealed that the majority of institutions are in the initial stages of LGPD implementation but also proposed numerous initiatives for adoption by federal public agencies (Tribunal de Contas da União, 2022).

Subsequently, we conducted an analysis of the questionnaire developed by the TCU. This evaluation allowed us to identify questions that had not been totally addressed in the original version of the checklist. These items were deemed essential for enhancing the checklist's capacity to support a more comprehensive assessment of LGPD compliance, particularly in areas where public institutions often face challenges. As a result, five new items were integrated into the checklist, numbered from S-13 to S-17, expanding its coverage. Table 1 presents the items added to the new version of LGPD-Check.

Table 1 – Enhancements in LGPD-Check

ID	Item Assessed
S-13	Does the system implement a process for registration, cancellation, and provisioning for access control?
S-14	Does the system have a formal process for registering and canceling users of systems that handle personal data?
S-15	Does the system have a formal process for granting or revoking access rights?
S-16	Does the system maintain an accurate and up-to-date record of users authorized to access information systems or personal data contained within them?
S-17	Does the system implement the protection of personal data both in transit (SSL) and at rest?

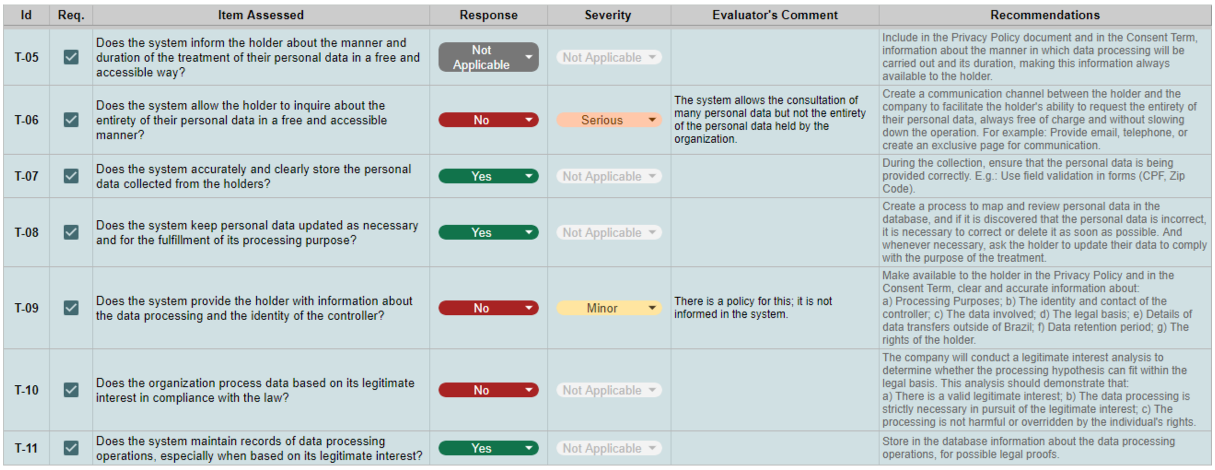
After improving the checklist, of the total 61 items, 47 were considered mandatory, while 14 were deemed non-mandatory. Additionally, the enhanced checklist items have been categorized according to what was previously defined by Mendes, Viana e Rivero (2021), comprising five categories: data transparency, holder consent, holder's rights, data security, and controller's responsibility.

The checklist represents a relatively cost-effective inspection technique, adaptable to various evaluation stages (LAITENBERGER; EMAM; HARBICH, 2001). However, its implementation may be perceived as labor-intensive due to the requisite process of defect identification. In this context, the adoption of tool-based support can significantly enhance the efficiency of the software inspection process.

For this reason, the artifact LGPD-Check was upgraded to a new version implemented in an online spreadsheet format to incorporate all items into the LGPD inspection checklist. This artifact will provide the necessary support for defect detection via a checklist, allowing for tracking completion and providing charts that illustrate the degree of non-compliance and system adherence. The enhanced LGPD-Check checklist is available in its entirety in Appendix D.

3.3 Application of LGPD-Check in Industry

In this Section, we provide an example of the checklist application for assessing software systems' adherence to LGPD quality attributes within a Government Office. This study aims to assess and improve an existing checklist proposed by Mendes, Viana e Rivero (2021), known as LGPD-Check, which evaluates software systems' compliance with the quality attributes specified by the Brazilian LGPD. The inspection checklist consists of multiple attributes distributed among several evaluation categories, including data transparency, holder consent, holder's rights, data security, and controller's responsibility. To evaluate the checklist's effectiveness, we applied the LGPD-Check within a government office, examining different web applications, followed by a focus group involving IT practitioners. This tool aims to support software development teams by providing a reliable and suitable checklist for Software Quality, facilitating the safe maintenance of user data.



Id	Req.	Item Assessed	Response	Severity	Evaluator's Comment	Recommendations
T-05	☑	Does the system inform the holder about the manner and duration of the treatment of their personal data in a free and accessible way?	Not Applicable	Not Applicable		Include in the Privacy Policy document and in the Consent Term, information about the manner in which data processing will be carried out and its duration, making this information always available to the holder.
T-06	☑	Does the system allow the holder to inquire about the entirety of their personal data in a free and accessible manner?	No	Serious	The system allows the consultation of many personal data but not the entirety of the personal data held by the organization.	Create a communication channel between the holder and the company to facilitate the holder's ability to request the entirety of their personal data, always free of charge and without slowing down the operation. For example: Provide email, telephone, or create an exclusive page for communication.
T-07	☑	Does the system accurately and clearly store the personal data collected from the holders?	Yes	Not Applicable		During the collection, ensure that the personal data is being provided correctly. E.g.: Use field validation in forms (CPF, Zip Code).
T-08	☑	Does the system keep personal data updated as necessary and for the fulfillment of its processing purpose?	Yes	Not Applicable		Create a process to map and review personal data in the database, and if it is discovered that the personal data is incorrect, it is necessary to correct or delete it as soon as possible. And whenever necessary, ask the holder to update their data to comply with the purpose of the treatment.
T-09	☑	Does the system provide the holder with information about the data processing and the identity of the controller?	No	Minor	There is a policy for this; it is not informed in the system.	Make available to the holder in the Privacy Policy and in the Consent Term, clear and accurate information about: a) Processing Purposes; b) The identity and contact of the controller; c) The data involved; d) The legal basis; e) Details of data transfers outside of Brazil; f) Data retention period; g) The rights of the holder.
T-10	☑	Does the organization process data based on its legitimate interest in compliance with the law?	No	Not Applicable		The company will conduct a legitimate interest analysis to determine whether the processing hypothesis can fit within the legal basis. This analysis should demonstrate that: a) There is a valid legitimate interest; b) The data processing is strictly necessary in pursuit of the legitimate interest; c) The processing is not harmful or overridden by the individual's rights.
T-11	☑	Does the system maintain records of data processing operations, especially when based on its legitimate interest?	Yes	Not Applicable		Store in the database information about the data processing operations, for possible legal proofs.

Figure 2 – Example of an evaluation process using LGPD-Check

For completion LGPD-Check, the evaluator, when starting a software inspection, must select one of three options in the 'Answer' column to evaluate the item: 'Yes', 'No', and 'Not Applicable'. If the evaluator determines 'Yes', it indicates that the item complies with the LGPD. By selecting 'No', the evaluator expresses that the item is defective or not compliant. If they choose 'Not Applicable', it means that the item is not inserted into the operational context of the company or is not related to the specific data treatment conducted by it. An example of this would be an organization that does not share data with foreign countries or does not process the personal data of children and adolescents. Figure 2 illustrates an example of an evaluation process using LGPD-Check.

As per Bastos et al. (2007), indicating the severity of the defect is the best strategy for prioritizing corrective action and its subsequent implementation. Thus, for each faulty item, it is up to the evaluator to denote the Severity Degree. The proposed checklist includes three severity degrees, adapted from the Nielsen scale (NIELSEN, 1994): Mild, Severe, and Catastrophic. With a low repair priority, the Mild degree impacts less critical data and minor functions. The Severe degree, with a high correction priority, affects the main functionalities and data, requiring short-term corrective actions. Finally, with mandatory correction, the Catastrophic degree severely impacts the system and requires immediate correction to minimize significant effects on the organization.

The 'Evaluator's Comment' column is an optional field, allowing it to be filled with any information about the item under evaluation. The evaluator is free to provide information such as the defect's location in the system for correction, who is responsible for the faulty functionality, who will correct it, and when it will be implemented, among other relevant comments.

Lastly, the checklist has a field dedicated to Recommendations for the items. These are optional suggestions for correcting or implementing the requirements of the LGPD law, based on some rules stipulated by the National Data Protection Agency of Brazil (ANPD), as well as systematic literature mapping carried out by Mendes, Viana e Rivero (2021). These authors sought to identify the attributes prescribed by law. The goal was to assist software developers in understanding the problem and searching for suitable solutions.

3.4 Feasibility Study of LGPD-Check

From March to July 2023, Neitzke et al. (2023) conducted a comprehensive study within a federal public agency, specifically the Electoral Regional Court of Maranhão (TRE-MA), an integral organ of the Federal Judiciary Branch. The institution's mission is encapsulated in the statement: *"Strengthen democracy through the electoral process"*. The primary mandate of TRE-MA encompasses the administration of the electoral process in its entirety, spanning from voter registration and election operations to the adjudication of matters pertaining to electoral processes and legislation.

Headquartered in the Capital (São Luís) and with jurisdiction throughout the Maranhão State, it is composed of seven Members (BRAZIL, 1988):

- Two judges among the judges of the Court of Justice;
- Two judges, among Judges of Law, chosen by the Court of Justice;
- A Federal Judge chosen by the Federal Regional Court of the First Region;
- Two judges among six lawyers of notable legal knowledge and moral integrity, appointed by the President of the Republic appointed by the Court of Justice.

The Regional Electoral Attorney, together with his/her substitute, will be appointed by the General Electoral Attorney from among the Regional Attorneys of the Republic in the State, or, where there is none, among the lifetime Attorneys of the Republic, for a term of two years (BRAZIL, 1993).

The feasibility study of LGPD-Check was applied within TRE-MA to evaluate the checklist's effectiveness, involving IT professionals responsible for different web applications, followed by a focus group meeting (NEITZKE et al., 2023).

The inspection protocol applied was based on the method suggested by Sauer et al. (2000), divided into four stages: planning, detection, collection, and discrimination. The participants used a checklist to inspect the computer systems of a federal public entity.

The aim of the evaluation was established based on the GQM (Goal Question Metric) objective definition template (BASILI; ROMBACH, 1988). The purpose of the study is to analyze the LGPD inspection checklist technique, with the intent to characterize it in terms of its feasibility about the indicators of effectiveness, efficiency, ease of use, usefulness, and intention to use from the perspective of industry professionals, in the context of software development projects.

The feasibility of the checklist technique was characterized based on the TAM (Technology Acceptance Model), which proposes that the perceived ease of use, intention, and utility of a technological tool determine the extent of user acceptance (DAVIS; BAGOZZI; WARSHAW, 1989). The TAM was chosen for this research due to its widespread acceptance in the academic community, its robust theoretical foundation for evaluating technology adoption, and its particular suitability for assessing novel tools in organizational settings where user perception directly impacts implementation success. This evaluation used three attributes: perceived ease of use, perceived usefulness, and perceived future use intention.

Besides a TAM-based approach, we conducted a focus group to capture both quantitative and qualitative insights. The TAM model offers a robust framework for evaluating user perception, while the focus group enables a more in-depth understanding.

3.4.1 Participants

The participants of the experience are professionals working in different IT departments within this organization. Eight professionals participated in this evaluation, all of whom are civil servants and have extensive experience in software development. Regarding their academic background, all of them are graduates of computing courses, with three having graduate degrees (specializations) and four holding a Master's degree in Computer Science. As for the knowledge about LGPD, only one of the participants considers their knowledge to be superficial. The rest have already participated in training provided by the organization, even working in the area of LGPD compliance. Each of the eight participants is assigned to a different department within the agency, working in the IT field. The list below presents each department along with the respective system evaluated by the inspector (NEITZKE et al., 2023):

- Data, Systems Development and Innovation Section (SEDIN): Authority registration control system;
- Information Security Management Section (SEGIN): Institutional website of the Court;
- Judicial Systems Support Section (SESJU): Guardião applications portal;
- Network Management Section (SERED): User registration for network and email access;
- Systems and Innovation Coordination (COSIN): Guardião applications portal;
- Training Section (SECAP): System for distance learning;
- User Support and Maintenance Section (SEASU): Service Desk management system.
- Web Management Center (WEB): Event management system;

These participants signed an Informed Consent form and filled out a Characterization Questionnaire, according to available in the Appendices A and B. The purpose of this consent form was to inform the participants that they would be part of a real industry experience related to inspections for compliance with the LGPD. The characterization questionnaire contained questions about (1) level of education and academic training; (2) experience in the current position; and (3) knowledge in software inspection and experience with the LGPD.

3.4.2 Resources

Concerning the materials used in the inspection, the following were prepared to support the inspectors:

- A presentation and general instructions about the checklist technique;
- A route specification that describes the activities carried out during the inspection;
- The online spreadsheet of the inspection checklist for the LGPD; and, finally,
- A questionnaire aimed at evaluating the applied technique;
- A digital collaborative cloud-based platform that allows users to collaborate in real-time by creating and sharing content on a shared virtual whiteboard. The focus group meeting employed this tool to conduct it.

3.4.3 Planning and Conduction

The defect detection task was individually executed by the inspectors, who initially had a seven-day deadline. However, given that the participants are industry professionals with working hours to comply with, they were granted fourteen days for completion. This timeframe included responding to the consent and characterization form, filling out the checklist, and finally, answering the technique evaluation questionnaire (NEITZKE et al., 2023).

Each inspector chose a familiar computational system to evaluate using LGPD-Check. Then they followed the script and judged each item. They could perform defect detection at the most convenient time, provided they fulfilled the activities and deadlines set. Within fourteen days, the inspectors filled out their spreadsheets and completed the consent, characterization, and post-inspection technique evaluation questionnaires. In summary, the script that contains the activities of the study is presented next:

1. Initially, all participants received an email with all information and links to the necessary materials;
2. In the second stage, the participants completed the consent form and characterization questionnaire, thus providing authorization for the research and answering several questions about their profile;

3. Next, the participant completed the checklist called "LGPD-Check", following the instructions provided carefully;
4. Upon completing the checklist, the participant proceeded to evaluate it by filling out the evaluation form, according to available in Appendix C;
5. Lastly, all participants were convened for a Focus Group meeting, where defects found in the inspections were discussed. This meeting also allowed for a discussion on the technique used and answering subjective questions with the aim to identify: (a) the central ease and difficulties encountered when using the checklist; (b) assess possible changes and improvements to the technique.

The evaluation checklist form was composed of objective questions based on the TAM model, an adaptation of the work of Davis, Bagozzi e Warshaw (1989). This was organized into three columns: the first column pertains to the question code, involving the perceived ease of use (EU), the perceived usefulness (UT); the last two questions focus on the perceived intention to use (IU). A general question presentation and a detailed analysis of the aspect under evaluation followed this.

The answers to the objective questions of the evaluation forms relating to the post-inspection technique were formulated based on the Likert scale (MCIVER; CARMINES, 1981), composed of four response alternatives: Strongly Agree (SA); Somewhat Agree (SWA); Somewhat Disagree (SWD); and Strongly Disagree (SD).

The focus group is a method widely employed in research, where a meeting with a group of people is arranged, with the aim of fostering interaction among the participants, where it is collectively possible to express their opinions in accordance with a swift and easy methodology (DEBUS, 1994). A typical focus group discussion involves between three to twelve participants, with a moderator leading and managing the dialogue. The moderator follows a set structure to keep the conversation on track (KONTIO; LEHTOLA; BRAGGE, 2004). In our focus group meeting, we conducted it by inviting all practitioners to join the experience. However, four could not participate due to travel, vacation, or medical issues.

A collaborative tool with an online digital whiteboard called *Jamboard* was utilized to facilitate more significant interaction among the participants. The participants had two minutes for each question posed to register their answers on digital post-its. During the drafting of the answers, these remained invisible to the others. However, once published, all the answers became visible to the group. Subsequently, a discussion about each question took place, aiming to debate the different perspectives of the checklist evaluators. Each participant had their name registered on the digital board. Thus, the participant responded on the Post-it corresponding to their color for each new question. Upon finishing their answers, the participants signaled by raising a hand in Google Meet. In this way, waiting the full two minutes would not be necessary if everyone finished earlier.

For a more fluid discussion, it was decided that each participant would have a specific moment to speak. It was also established that if a participant agreed with the viewpoint of another, they could simply place their Post-it next to the participant's with whom they agreed, thus demonstrating their agreement.

The execution of the focus group followed guidelines linked to four fundamental aspects:

- **Duration**: The focus group should be concise, not exceeding two hours, to avoid fatigue and mental wear, as this technique induces intense discussions, which can leave the participants exhausted (MAZZA; MELO; CHIESA, 2009). Considering this, we limited the number of questions, making the meeting relatively straightforward.
- **Location**: The meeting was held via an online conference using the Google Meet communication service.
- **Recording**: The session was recorded to document the entire study process and served as material for the focus group transcription.
- **Team**: The team was composed of two researchers who performed the roles of coordinator and observer of the study.

As stipulated by Dall'Agnol e Trench (1999), the coordinator and observer should establish effective communication with the participants, demonstrating complete mastery of the study's purposes without allowing the discussion to deviate from the study's context.

The following questions were discussed during the meeting:

1. What are the main advantages that your institution can gain through the use of the checklist?
2. What modifications would you suggest to the checklist to improve fault detection in systems?
3. Were the recommendations beneficial in understanding the issues and assisting in the resolution of possible defects?
4. Were the instructions provided for the completion of the checklist helpful?
5. What were the simplest and most complex points when employing the checklist during the inspection?

All data from the post-inspection technique evaluation form have been compiled and will be discussed in the following section. In addition, the next section will present the results obtained from the TAM model (DAVIS; BAGOZZI; WARSHAW, 1989) and the qualitative evaluation, which includes the performance analysis of the inspection checklist usage and the outcomes of the focus group meeting.

Table 2 – Assessment Questionnaire

Ease of use:	
EU-1	The checklist was clear and easy to understand.
EU-2	In general, I find it easy to find defects or problems in a system with the checklist.
EU-3	The checklist required little mental effort.
Utility:	
UT-1	I think the checklist is useful for finding defects or problems in the system.
UT-2	The checklist used improves my productivity by identifying defects or problems in the system.
UT-3	The checklist allows me to perform the system inspection more quickly.
Intention of use:	
IU-1	I intend to use the checklist to find defects or problems in the system in the future.
IU-2	I would recommend the checklist to other development teams.

3.4.4 Results and Analyses

In this section, the results of the LGPD inspection checklist assessment are discussed using two perspectives: (1) Analysis with the TAM model, focused on the objective data collected from the post-inspection evaluation form; and (2) Qualitative Analysis, which consists of an analysis of the inspectors' comments, based on the data collected in the focus group meeting about the checklist.

3.4.5 Use of the TAM Model for Analysis

In the evaluation conducted using the TAM model, we considered the objective responses from the post-inspection evaluation form. This form was employed to evaluate LGPD-Check regarding ease of use, usefulness, and intended use. After utilizing the checklist, the inspectors completed it according to their level of agreement with the statements based on their perception. Table 2 displays the questions, while figure 3 visually represents this data.

It was observed that 37.5% of the inspectors strongly agree (SA) on the clarity and understanding of the checklist, while 62.5% somewhat agree (SWA). The majority of inspectors fully agree on the ease of defect detection. However, 12.5% of the inspectors somewhat disagree (SWD) that the technique requires little mental effort.

Regarding perceived utility, there was a consensus among the inspectors that the checklist, in general terms, makes system inspection faster. More than half of the inspectors fully agree that the checklist contributes to increasing their productivity in defect identification. Finally, 87.5% of the inspectors strongly agree that the checklist is helpful in detecting system defects. Figure 3 presents data on the perceived intention for future use by the inspectors who used the checklist.

Regarding the perceived intention for future use, all inspectors expressed the intention to use the checklist in the future. More than half of the inspectors intend to use the checklist

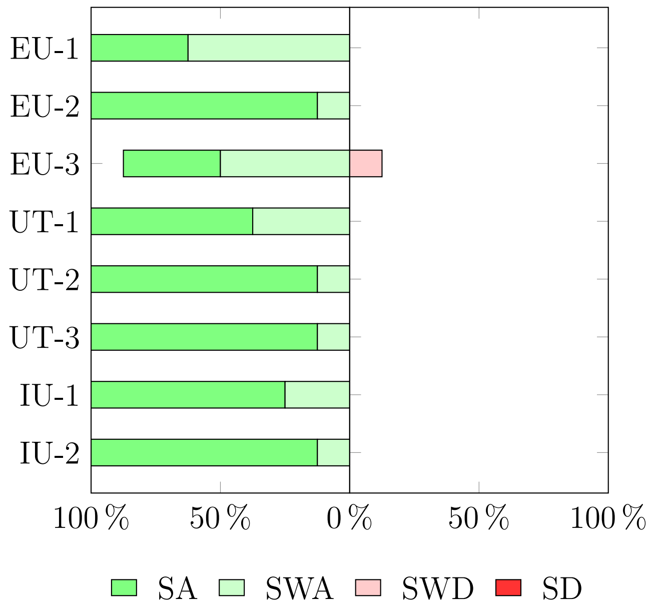


Figure 3 – Results of post-inspection evaluation form

in other computer systems to assess their compliance with the LGPD. Moreover, 87.5% of the inspectors would recommend the checklist to other companies that process data and wish to evaluate their systems' compliance with the LGPD.

According to the results from the three perspectives - ease of use, utility, and intention of use - it can be concluded that most inspectors fully agree that the checklist is easy to use, that it is beneficial for defect identification, and that they intend to use it in the future. However, some inspectors believe that the checklist requires a significant mental effort to complete the verification items aimed at the system's compliance with the LGPD.

3.4.6 Qualitative Analysis

The qualitative analysis considered the data collected during the focus group meeting with four participants. Several issues were raised and discussed with the aim of better understanding the most significant challenges and benefits of using the evaluated checklist and its artifacts, as well as any potential changes or improvements suggested by the participants.

All inspector responses were originally crafted in Portuguese. However, we have made a concerted effort to translate them using the most precise terminology possible, with the aim of maintaining the integrity of the original feedback. The first question brought to the meeting was as follows: *What are the main advantages a public agency can gain from using the checklist?*

- *Inspector I-01: "It will facilitate understanding of the existing requirements in the LGPD (General Data Protection Law), which will aid in adherence to the law."*
- *Inspector I-02: "Efficiency and practicality in the analysis, allowing for a more complete check of the system, in order to decrease the chance of error or overlooking an important point."*

- *Inspector I-03: "It is possible to assess the adherence of systems to the principles of the LGPD and identify areas for improvement."*
- *Inspector I-04: "It can help to have a set of guidelines related to the LGPD to be complied with by the system, which I believe is not easy to understand."*

The opinions of the four inspectors reveal that the checklist can highlight gaps in systems to identify possible defects, clarify project doubts concerning the law, and assess the adherence of software to the principles of the LGPD, identifying areas for improvement.

The second question pertains to some issues encountered in using the checklist: *What modifications would you suggest to the checklist to enhance the detection of flaws in systems developed by public agencies?*

- *Inspector I-01: "Some questions should be posed from the business manager's standpoint."*
- *Inspector I-02: "Link the checklist item with the law requirement. So if the law changes, I can alter the item on the checklist more easily."*
- *Inspector I-03: "If there were a way to link the items with the article in the regulation, I think that would be interesting."*
- *Inspector I-04: "Better detail the options for the severity field to assist in defining this item."*

The first suggestion for improvement is to create specialized checklists according to the application area, providing specific versions for different evaluators, such as the controller, the data subject, or the software developer. Two inspectors also suggested that the checklist include the reference to the article of the LGPD that is being addressed with each item. Finally, one inspector offered more detailed explanations on how to classify the severity of an item when it is not met.

The next question addresses the usefulness of the recommendations column: *Was the recommendations column beneficial for understanding the issues and assisting in the resolution of possible defects?*

- *Inspector I-01: "Yes. It greatly assisted in understanding the issues."*
- *Inspector I-02: "Yes. In my case, as I am not well acquainted with the regulation, it was essential for me to be able to respond and understand in practice what the item referred to."*
- *Inspector I-03: "Yes, because it detailed the item to be answered, indicating what the evaluated system should meet."*
- *Inspector I-04: "Yes. I think there should be more examples or templates of documents for the recommendations."*

According to the inspectors, the recommendations listed in the checklist completion spreadsheet were useful and exceeded expectations. One of the evaluators suggested the inclusion of document templates for the solutions pointed out in the recommendations.

Regarding the support materials, the meeting asked: *Were the guidelines provided for completing the checklist beneficial?*

- *Inspector I-01: "Yes. They were sufficient."*
- *Inspector I-02: "Yes. They were sufficient."*
- *Inspector I-03: "Yes, clear and concise."*
- *Inspector I-04: "Yes, it was sufficient."*

Indeed, there was a concern about facilitating the inspection process of the checklist, the existing functionalities, and even the checklist artifact itself, making it quite intuitive so that inspectors could fill it out accurately and swiftly. A note was made regarding the evaluator's comment field, which was initially planned to be optional; however, some inspectors suggested that it should be mandatory in some instances.

Finally, the discussion turned to the ease and difficulties encountered during the inspection. The question asked was: *What were the simplest and most complex points when employing the checklist in the context of a public agency?*

- *Inspector I-01: "I see the unequivocal registration of the user's consent as something critical for the business."*
- *Inspector I-02: "Complex: the lack of detailed knowledge of the Law."*
- *Inspector I-03: "Simple: It provides an objective way to evaluate the systems. Complex: it is necessary to be well acquainted with the agency's regulations on the subject."*
- *Inspector I-04: "Simple: I think the definitions of the items and the recommendations are easier to understand because public servants have training in LGPD."*

The checklist, derived from a regulation document, covers intricate matters regarding the law. Nonetheless, its purpose is to assist inspectors in identifying weaknesses in their systems for pinpointing non-adherence and rectifying it as promptly as possible. Most of the inspectors had an intermediate understanding of the LGPD and were encouraged to delve deeper into the topic. For some participants, the checklist served as a guide for better compliance with the LGPD.

Overall, the results indicate that the LGPD inspection checklist technique can be applied in a real industry context to evaluate software systems for their adherence to the law and fulfills its objective in defect detection. However, the qualitative results indicate that there are still possibilities for improvement.

3.4.7 Implications for Practice

According to their familiarity and professional arrangement, each participant chose a computational system from the agency to inspect it. Thus, everyone had the necessary knowledge to judge each item of the LGPD-Check as compliant, non-compliant, or not applicable to the case. In the event of non-compliance with any item, the evaluator defined the severity of the defect, allowing the prioritization by criticality when resolving each issue.

Evaluator I-01, assigned to the SECAP, evaluated the agency's software for managing distance learning. According to his evaluation, the software adheres to 46% of LGPD's quality attributes. However, fundamental LGPD criteria need to be more compliant, such as the system not allowing the holder to provide their consent transparently and autonomously to process their data and also not informing about all their rights in consent.

Assigned to SERED, evaluator I-02 inspected a user registration software for network and institutional email access. Among the defects found, the lack of information about the purposes of personal data processing available to the holder stands out. Despite this, the evaluated system obtained the second-highest compliance rate among those considered, reaching a percentage of 53%.

Evaluator I-03, assigned to SEGIN, evaluated the institutional website of the agency. Many checklist items did not apply to the context, and a compliance rate of 29% was achieved. One of the most critical improvements to be made is the lack of a mechanism to provide a complete electronic copy of personal data to the holder. It was also reported that the system does not allow holders to update their personal data.

Evaluator I-04, assigned to COSIN, inspected an integrated authentication system called Guardian, achieving a compliance rate of 52% to LGPD. Although it was the software with the best index among those evaluated, it will still be necessary to implement a formal process for registering and canceling users who process personal data.

The WEB department, where inspector I-05 is assigned, is responsible for developing the organization's event system. According to the inspection carried out by the evaluator, the system is 39% compliant with LGPD. Among the defects found, there is a lack of a precise and updated registration mechanism for users who have been authorized to access personal data stored in the system.

Evaluator I-06, assigned to SEASU, evaluated the call registration software used by the IT Central, responsible for being the single entry point for users to request information technology services. It is essential to highlight that all items related to the category of holder consent were pointed out as not adhering to LGPD, therefore requiring urgent corrective actions to adapt the evaluated system. Regarding the LGPD compliance rate, it was 29% of adherence.

Evaluator I-07, assigned to SESJU, inspected the agency's applications portal and achieved a 45% adherence rate to LGPD. Many defective items were pointed out, including the impossibility of deleting the holder's personal data upon request, as well as not removing the holder's personal data after the end of their treatment.

Finally, inspector I-08, assigned to SEDIN, applied the LGPD-Check on a software named Corau, a system responsible for controlling the records of authorities linked to the agency. Many items in non-compliance were pointed out, generating a 38% compliance rate to LGPD. The priorities for correction are the formalization of data processing purposes in the organization and the implementation of an interface for the holder to inquire about the entirety of their personal data in an accessible manner.

Figure 4 displays the rate of compliant and defective items according to evaluations performed by each inspector.

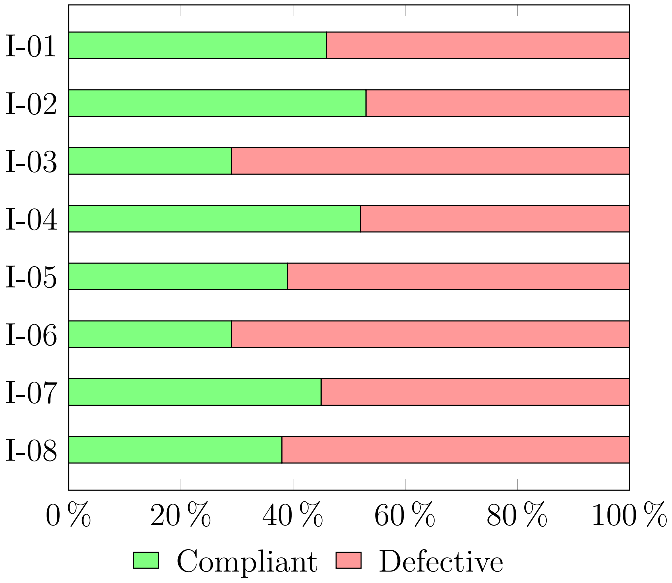


Figure 4 – Rate of compliant and defective items

As a significant benefit to the organization, this practical application of the LGPD-Check allowed for the structuring of tasks to enhance compliance with the LGPD. This occurred because the developers responsible for each evaluated system included the most critical defective items in their development backlog. These items will subsequently be prioritized and allocated in future sprints, resulting in an increase in the government office's software compliance index with personal data protection standards.

3.4.8 Threats to Validity

In all studies, there are potential threats that can impact the validity of the results. The threats associated with this study are presented below and classified into four categories: internal validity, external validity, conclusion validity, and construct validity.

Regarding internal validity, time measurement is a potential threat. There is no guarantee that the reported time was indeed measured accurately. Despite this, participants were instructed to be as precise as possible in their measurements to minimize errors. Another internal threat was related to defect discrimination. The inspectors, being individuals with reasonably deep knowledge of the system and with limited time to conduct the meeting, may have influenced the analysis.

In terms of external validity, the industry professionals analyzed in the literature and in this study have knowledge that ranges from reasonable to advanced about LGPD. To mitigate this threat to validity, a list of item implementation recommendations was added to the checklist, which facilitates the practical understanding of the regulation.

Regarding conclusion validity, the biggest threat is the sample size. The study has a small number of participants, which is sub-optimal from a statistical viewpoint. Due to this limitation, the results obtained in the research should be considered indicative, not conclusive.

Finally, construct validity relates to the definition of the indicators used to characterize the proposed technique. The indicators adopted in this study, which include the TAM model, are commonly used in studies investigating defect detection techniques. Moreover, we did not evaluate the adapted TAM instrument, since the changes were minor in the text of the items (change in the name of the technology and its goals). Also, our focus was on the LGPD-Check checklist, and validating the TAM instrument would require more subjects within our organization.

3.5 Final Considerations

Aiming to support software development teams, Neitzke et al. (2023) presents an improvement and evaluation of a checklist for inspecting the compliance of computer systems with the Brazilian General Data Protection Law. The initial technique was proposed by Mendes, Viana e Rivero (2021) and was refined based on comments from computing experts and through a peer review. Finally, this investigation seeks to evaluate the feasibility of using LGPD-Check by industry professionals within a Government Office.

Industry IT professionals acted as inspectors and used the checklist with the intention of identifying potential flaws in their organizations' systems. According to the analysis by the TAM model, from the data obtained through post-inspection forms, the technique proved to be accessible and valuable for most inspectors to identify flaws and allow better compliance with the requirements imposed by the law. Others agree but note that the checklist requires some mental effort. However, most inspectors intend to use the checklist in the future and would recommend it to colleagues.

Subsequently, a qualitative analysis was conducted, which collected data from the focus group meeting with participants and discussed the presented technique's strengths and weaknesses. The results indicated its potential for evaluating the software systems' adherence to LGPD quality attributes with ease from the point of view of software development practitioners within a government office. However, opportunities for improvement were identified, such as creating document templates for each recommendation and linking each question to its respective article in the law, thereby clarifying the item's origin.

Evaluating the impact on the organization, the utilization of the LGPD-Check had a significant positive impact. The application of this exploratory procedure permitted planning tasks in order to improve compliance with the LGPD. This was achieved by the developers of each evaluated system incorporating the most crucial defective elements into their development backlog. As a result, these items will be given priority and addressed in future sprints, leading to a considerable improvement in the government office's software compliance with personal data protection regulations.

To continue the process, we will implement the improvements suggested during the evolution process and conduct a new assessment of the LGPD-Check. It is hoped that the results achieved in this paper could be used to improve the current state of research on compliance with the LGPD and software quality. It is also expected to support software development teams by providing a more reliable, robust, and suitable checklist for use by the software industry, facilitating the safe maintenance of personal data.

4 LGPD-Check Upgrade

Following the feasibility study of the checklist presented in the previous chapter, an upgraded version of the LGPD-Check was developed. Each checklist item underwent a review, incorporating feedback and observations gathered from the prior study. This process aimed to refine the checklist and ensure its alignment with both the LGPD's legal requirements and practical applicability in real-world scenarios.

In addition to reviewing the checklist items, specific templates were created for each item of the LGPD-Check. By offering ready-to-use templates, such as sample policies, code snippets, or step-by-step guidelines, these templates bridge the gap between theoretical legal requirements and their practical implementation, making compliance more accessible to developers and organizations. Consequently, these examples and insights promote a comprehensive understanding of the data protection requirements mandated by the LGPD.

Furthermore, the templates simplify the inspector's role by providing a structured framework for evaluating and detecting non-conformities. This approach reduces the subjectivity of inspections and ensures that relevant aspects of LGPD compliance are systematically covered.

4.1 Improvements Implemented in LGPD-Check

The enhanced version of the LGPD-Check framework represents an advancement in terms of practicality and usability. The incorporation of templates into the checklist offers a practical solution for addressing non-conformities with LGPD requirements. These templates function as guides, providing evaluators and organizations with valuable resources to identify non-compliances and implement necessary improvements.

The templates added to LGPD-Check were developed through exploratory research and industry examples to address the diverse requirements of each checklist item, varying in format and complexity. These templates contain a range of resources, including policy drafts, code snippets, guides, and processes, as well as practical insights and recommendations that facilitate compliance with the legal provisions established by the LGPD.

For low-level items, the templates offer detailed and structured guidance, capable of directing the solution through configurations and source code examples. Contrariwise, for high-level items, examples of standards, policies, forms, and messages are provided. For items that can be addressed simply through recommendations, aiming to facilitate and guide the adjustment process, the templates were developed as 'Additional Guidance' to those already present in the 'Recommendations' column of LGPD-Check.

Table 3 presents a description of the types of models associated with each LGPD-Check item. For a complete view of all models, it is recommended to consult Appendix E, where they are available in their entirety.

Table 3 – Templates in LGPD-Check

Item	Template Type
T-01	Draft of Privacy Policy and Consent Terms
T-02	Legal Basis for Personal Data Processing
T-03	Purposes of Data Processing
T-04	Step-by-Step Guide for Reviewing Consent and Implementing Changes
T-05	Method and Duration of Data Processing
T-06	Personal Data Access Request Form
T-07	Sample Source Code
T-08	Structure of a Personal Data Mapping and Review Process
T-09	Sample Source Code
T-10	Illustrative Step-by-Step Guide
T-11	Sample Source Code
T-12	Topics for a Report on Data Processing Operations
T-13	List of Best Practices and Techniques for Anonymization and Pseudonymization
T-14	Model for Data Collection and Processing Notice
C-01	Recommendations and Guidance
C-02	Recommendations and Guidance
C-03	Sample Source Code
C-04	Sample Source Code
C-05	Sample Source Code
C-06	Additional Guidance
C-07	Additional Guidance
C-08	Draft of Consent Form for Personal Data Processing
D-01	Recommendations and Guidance
D-02	Additional Guidance
D-03	Recommendations and Guidance
D-04	Additional Guidance
D-05	Recommendations and Guidance
D-06	Recommendations and Guidance
D-07	Additional Guidance
D-08	Recommendations and Guidance
D-09	Additional Guidance
D-10	Additional Guidance
D-11	Example Message Explaining the Necessity of Data Collection for Service Provision
D-12	Additional Guidance
D-13	Additional Guidance
D-14	Additional Guidance
D-15	Additional Guidance
S-01	Insights for Implementing Security Mechanisms

Item	Template Type
S-02	Recommendations and Guidance
S-03	Example Content for Inclusion in Privacy Policy
S-04	Example Scripts for Security Configuration Implementation
S-05	Examples of Security and Audit Configurations in Databases
S-06	Additional Guidance
S-07	Additional Guidance
S-08	Examples of Practices and Technologies
S-09	Additional Guidance
S-10	Additional Guidance
S-11	Draft Privacy and Security Incident Correction Plan
S-12	Additional Guidance
S-13	Additional Guidance
S-14	Additional Guidance
S-15	Additional Guidance
S-16	Examples of Audit Configurations in Databases
S-17	Additional Guidance
R-01	Additional Guidance
R-02	Additional Guidance
R-03	Additional Guidance
R-04	Example of a Data Protection Impact Assessment Document
R-05	Additional Guidance
R-06	Additional Guidance
R-07	Additional Guidance

A practical example of this approach is the model related to item **C-08: Does the system inform the data subject about all their rights in the consent declaration?**. This item aims to assess whether the system clearly and comprehensively communicates all the data subject's rights in the consent declaration, as required by the LGPD. To assist in addressing this non-conformity, the template presents a draft consent form for personal data processing. Consequently, this document can be easily adapted to the specific context of the institution.

Consent Declaration for the Processing of Personal Data

Dear Data Subject,

This Consent Declaration aims to inform and obtain your consent for the processing of your personal data in accordance with the General Data Protection Law (LGPD - Law No. 13,709/2018). Below, we describe in clear and accessible terms how your data will be used and your rights as a data subject.

1. Collection of Personal Data The personal data collected may include, but is not limited to: name, address, email, phone number, CPF, banking information, and other necessary details for the provision of our services.

2. Purpose of Data Processing The collected data will be used for the following purposes:

- Describe specific purposes, such as: service provision, communications, compliance with legal obligations, etc.

3. Data Sharing Your data may be shared with:

- List recipients, such as: business partners, service providers, competent authorities, etc.

4. Rights of the Data Subject Under the LGPD, you have the following rights regarding your personal data:

- **Confirmation of Processing:** The right to know if your data is being processed.
- **Access to Data:** The right to access your personal data processed by us.
- **Correction of Incomplete, Inaccurate, or Outdated Data:** The right to request the correction of your data.
- **Anonymization, Blocking, or Deletion:** The right to request the anonymization, blocking, or deletion of data that is unnecessary, excessive, or not compliant with the LGPD.
- **Data Portability:** The right to receive your data in a structured and interoperable format.
- **Deletion of Data Processed with Consent:** The right to request the deletion of data processed based on your consent, except as provided by law.
- **Information on Data Sharing:** The right to know which public and private entities your data is shared with.
- **Information on the Option to Not Consent:** The right to be informed about the possibility of not providing consent and the consequences of this decision.
- **Revocation of Consent:** The right to revoke consent at any time through an explicit request.

5. Data Security We adopt appropriate technical and organizational security measures to protect your personal data from unauthorized access, loss, destruction, or alteration.

6. Contact for Exercising Rights To exercise any of your rights or if you have questions about the processing of your personal data, please contact us at: [`youremail@domain.com`].

7. Changes to this Consent Declaration We reserve the right to update this Consent Declaration periodically. Any changes will be communicated to you through our usual communication channels.

By clicking the button below, you agree to the processing of your personal data as described above.

The following section will present a detailed evaluation of the recently integrated models in an industrial context. This analysis seeks to examine the effectiveness and applicability of the recommendations and templates in real-world scenarios, as well as identify opportunities for future refinements.

4.2 Evaluation of Templates in Industry

This chapter aims to detail the evaluation process of the recommendations and templates included in the new version of LGPD-Check. Section 4.2.1 discusses the overall study planning. Section 4.2.2 characterizes the participant profiles. Section 4.2.3 describes the method used to conduct the study. Section 4.2.4 presents the evaluation's qualitative results based on volunteers' participation in a focus group directed at the proposed templates. Section 4.2.5 discusses the implications of the findings. Finally, Section 4.3 provides the final considerations of the chapter.

4.2.1 Study Planning

The main objective is to gather detailed insights into the applicability, effectiveness, and suggestions for improving LGPD-Check based on the participants' experiences. Through a collaborative and semi-structured discussion, the study aimed to identify the strengths and weaknesses of the templates and recommendations of each checklist item, understand the difficulties encountered during their application, and collect practical suggestions for enhancements.

The schedule began with an introductory presentation of LGPD-Check and its templates on June 18, 2024. Participants were allowed to evaluate two systems from June 18 to June 24, 2024. The systems assessed were *Coleta* and *Mercado Solidário*, both developed within the context of UFMS. Subsequently, on June 25, 2024, we conducted a focus group session remotely via Google Meet. Considering that the focus group technique can generate intense and potentially exhausting discussions for participants (MAZZA; MELO; CHIESA, 2009), we planned the meeting duration not to exceed two hours to minimize fatigue and mental strain. Therefore, we limited the number of questions to keep the session concise, with the expectation of completing the meeting within an hour and a half.

The following section will focus on characterizing the study participants. It will provide details about their profiles, including professional information and their familiarity with the topics addressed in the LGPD-Check evaluation process.

4.2.2 Participants

The study was conducted remotely and involved students from the Federal University of Mato Grosso do Sul (UFMS). Ten participants, all professionals working in the software engineering industry, were selected to evaluate the recommendations and templates incorporated into the LGPD-Check. The selection process followed specific criteria to ensure the relevance and reliability of the evaluations, prioritizing professionals with practical experience in the field.

We formally invited participants as described in Appendix F. They received detailed instructions about the study, provided in Appendix G. Before engaging in the activities, all participants signed a Free and Informed Consent Form (TCLE), ensuring they were aware of the study's objectives, procedures, and implications (Appendix A). Subsequently, they completed a characterization questionnaire (Appendix B), which collected relevant information, such as age, gender, education level, professional area, years of experience, and prior knowledge of the LGPD.

All male participants were between 19 and 27 years old and held undergraduate degrees in computing-related fields. Analysis of the collected data revealed that all participants had some prior knowledge about the LGPD, a prerequisite for participation in the study. Table 4

Table 4 – Participant Profiles of the Evaluation Study

Inspector	**Current Position or Role**	**Experience**
I-01	Software Engineer	2 years
I-02	Backend Developer	2 years
I-03	Mobile Developer	3 years
I-04	Tester	4 months
I-05	UX Researcher + Front-end Developer	1 year
I-06	Front-end Developer	1 year
I-07	Project Manager and Developer	1 year and 6 months
I-08	Front-end Developer	2 years
I-09	Software Engineer	18 months
I-10	Volunteer Participant	5 years

presents the professional profiles of the participants, including their years of experience in the software engineering domain.

The research team also included two researchers, who assumed the roles of study coordinator and observer. According to the methodological guidelines proposed by Dall'Agnol e Trench (1999), the coordinator and observer are responsible for maintaining effective communication with participants while demonstrating a complete understanding of the study's objectives. Furthermore, they ensure that discussions remain focused on the study's context, avoiding deviations that could compromise the results.

This section underscores the selection of participants and the structured roles of the research team, emphasizing the adherence to methodological rigor and ethical standards essential for obtaining reliable results. The following section will detail the evaluation method employed in the study, outlining the procedures, instruments, and criteria used to assess the proposed recommendations and templates.

4.2.3 Evaluation Method

The evaluation process involved inspecting two internally developed systems at UFMS: the **Coleta** system and the **Mercado Solidário** system, using the LGPD-Check framework. Each evaluator received a list of at least 12 items for the comprehensive assessment of recommendations and templates, as outlined in Table 5. Participants received one week to conduct their evaluations individually from June 18 to June 24, 2024.

All items from the LGPD-Check were distributed among the 10 participants involved in the study, ensuring comprehensive coverage of all aspects addressed in the checklist. To mitigate potential threats to conclusion validity, the study employed a distribution strategy where at least two inspectors independently reviewed each item. This approach enhanced the reliability and quality of the conclusions drawn.

During the initial evaluation phase, the participants analyzed the systems individually, following the guidelines provided. The aim was to test the applicability, clarity, and completeness

Table 5 – Minimum Items Evaluated by Inspectors

Inspector	**Minimum Items Evaluated**
I-01	From item T-01 to T-12
I-02	From item T-07 to C-04
I-03	From item T-13 to D-02
I-04	From item C-05 to D-08
I-05	From item D-03 to D-14
I-06	From item D-09 to S-05
I-07	From item D-15 to S-11
I-08	From item S-06 to S-17
I-09	From item S-12 to R-07
I-10	From item R-01 to R-07 and from T-01 to T-05

of the recommendations and templates within a real-world context. This phase allowed participants to form preliminary opinions on the usability and effectiveness of the LGPD-Check framework.

Following the individual evaluation, a focus group meeting was conducted remotely via Google Meet on June 25, 2024. The meeting was semi-structured and guided by pre-defined questions to facilitate the discussion and evaluation of the recommendations and templates.

The session began with a brief introduction and welcome to the participants, including the presentation of the moderator and observer, a description of the meeting's objectives, and an explanation of the focus group dynamics, emphasizing the assurance of confidentiality and anonymity. Following this, an introduction to the LGPD-Check was provided, covering the project's scope, the objectives of the checklist, and the structure of its categories and templates. The main discussion was divided into five thematic blocks: Data Transparency, User Consent, User Rights, Data Security, and Controller Responsibilities, each involving the presentation of relevant items and targeted questions to assess clarity, applicability, and suggestions for improvement. Finally, there was a space for general discussion and final feedback, followed by closing remarks expressing gratitude and providing contact information for any additional contributions. The meeting agenda is detailed in Appendix H.

Participants had two minutes to type their answers in the Google Meet chat before sharing them aloud. Once posted, responses became visible to the group, initiating a collective discussion. Every participant could share their viewpoint, guaranteeing a fair allocation of speaking time and encouraging a more inclusive conversation.

The focus group's objective was to acquire comprehensive feedback regarding implementing LGPD-Check. It emphasized the recommendations and templates' strengths and limitations while eliciting actionable suggestions for enhancement. This participatory approach validated the framework's relevance and facilitated the refinement of its components based on real-world insights.

The following section will present the qualitative evaluation results, analyzing the insights, deficiencies, and suggestions provided by the participants. These findings will contribute to further refinement of the LGPD-Check framework, enhancing its applicability and effectiveness in promoting compliance with the General Data Protection Law.

4.2.4 Discourse Analysis

All focus group participants' contributions were recorded to capture the key insights and suggestions shared during the session. These records were organized according to the five categories that structure the LGPD-Check framework: Data Transparency, User Consent, User Rights, Data Security, and Controller Responsibilities.

Based on these records, we coded to identify and group similar themes and items, enabling a more structured and coherent analysis of the contributions. The use of codes is intended to assist in recognizing patterns, inconsistencies, and improvement areas associated with the analyzed recommendations and templates.

Table 6 presents the contributions related to the "Data Transparency" category, highlighting the perceptions and challenges identified by participants during the evaluation of LGPD-Check. Some participants reported initial difficulties in analyzing the questions, primarily due to the complexity or abstraction of the text in certain items. However, the clarity of the questions was noted as a positive aspect, indicating that, despite initial challenges, most evaluators found the items understandable. The ease of evaluation was also emphasized, mainly due to the support provided by the recommendations and templates. On the other hand, participants mentioned challenges in distinguishing applications when specific questions could apply to different contexts. These observations underscore both the quality and the areas for improvement needed in the checklist to accommodate diverse evaluator profiles.

Table 6 – Results: Data Transparency

Aspect	**Contributions**
Initial Analysis Difficulty	I-01: "I admit that it took me a while to analyze the questions." I-01: "It took me a while to analyze the questions because it had been some time since I last worked on the project..." I-02: "There were some questions that I had to think a bit more about before answering." I-03: "I also found the text a bit abstract in some questions."
Clarity of Questions	I-01: "The questions themselves were very clear. I didn't have difficulty understanding any specific item, for example."

Aspect	**Contributions**
Ease of Evaluation	I-01: "The questions made it much easier..." I-01: "But the questions provided a smoother flow to carry out the evaluation." I-02: "The recommendations and templates helped me understand exactly what that specific topic was about."
Difficulty in Separating Applications	I-03: "I had difficulty separating the applications because I noticed that some questions fit one application but not the other..."

Table 7 presents the results related to the "User Consent" category. It highlights the participants' feedback on the clarity of the questions, which were well understood without requiring additional analysis. However, it also identifies a perceived gap in providing more detailed definitions and explanations, suggesting the need for greater contextualization to enhance the understanding of the questions and recommendations.

Table 7 – Results: User Consent

Aspect	**Contributions**
Focus on Testing Development	I-04: "I'm not very involved in this part because I'm more focused on load testing and exploratory testing."
Clarity of Questions	I-02: "I was able to understand the questions very well, so much so that I didn't even need to go back to the recommendations I mentioned earlier."
Lack of Definitions and Explanations	I-05: "I felt the absence of a brief definition, explanation, or implications, as seen in previous templates."

Table 8 presents the results related to the "User Rights" category in LGPD-Check, highlighting factors such as participants' prior familiarity with the LGPD, which facilitated the evaluation, and the confusion caused by more abstract questions. Additionally, specific cases within the evaluated systems were noted where certain rights were less applicable due to the presence of intermediary users, contrasting with scenarios of direct use by end users. Participants also reported uncertainties regarding the distinction between public and private data and the absence of definitions and explanations that could enhance the understanding of the presented questions.

Table 8 – Results: User Rights

Aspect	**Contributions**
Familiarity with LGPD	I-06: "The prior knowledge we had about LGPD helped a lot."
Confusion with Abstract Questions	I-03: "I found some questions abstract."
Specific Cases in Evaluated Systems	I-03: "In the data collection application, these rights are not as visible because there's an intermediary user." I-03: "In the market, this is more commonly applied because the user interacts directly with the application, so some things apply automatically."
Confusion About Public and Private Data	I-07: "In the case of legal entities, data like tax ID numbers and registration details are truly public... This also confused me." I-07: "I initially didn't understand D09, which caused some confusion, but it's all clear now."
Lack of Definitions and Explanations	I-05: "I felt the absence of a brief definition, explanation, or implications, as seen in previous templates."

Table 9 presents the results related to the "Information Security" category, highlighting aspects such as the clarity of the questions, the complexity of the recommendations, and the support provided by the templates. Participants noted that the questions were easy to understand, while another participant pointed out the density of the recommendations due to the inclusion of multiple techniques. Furthermore, the templates were praised for covering critical aspects such as encryption and secure protocols and for facilitating implementation using more appropriate frameworks compared to *Portugol*, a beginner-friendly programming language in Portuguese, designed to teach fundamental programming concepts using simple, human-readable commands. Finally, the importance of quantifying the criticality of system impacts was emphasized, along with the need for practical examples or specific guidance.

Table 9 – Results: Information Security

Aspect	Contributions
Clarity of Questions	I-07: "I had no difficulty understanding the questions. I think they were very clear and easy to comprehend." I-08: "I thought they were very clear."
Complexity of Recommendations	I-06: "Maybe it has too many details, as it includes questions about appropriate techniques, listing over 10 different techniques."
Assistance from Templates	I-06: "I found this question very interesting because it covers many aspects like encryption, secure protocols, safe storage, and frameworks." I-09: "The attached template you provided was very helpful."
Framework Use Instead of Portugal	I-06: "Using a language more effective than *Portugol* makes a difference since there's a significant gap in showing this in *Portugol.*" I-09: "I liked how it was presented, instead of *Portugol*, as it makes implementation easier."
Criticality Importance	I-07: "It's about quantifying how much I think this question impacts the system or overall."
Examples and Guidance Elaboration	I-08: "There's a need to structure the question by providing an example or guidance on which technique to use."

Table 10 presents the contributions related to the "Controller Responsibility" category, highlighting the ease of response attributed to the team's internal organizational process. According to the participant, the well-structured context and familiarity with the team's internal processes significantly facilitated the completion and evaluation of the proposed items. This feedback underscores the importance of a clear and well-defined organizational environment for effectively applying the checklist.

Table 10 – Results: Controller Responsibility

Aspect	Contributions
Ease of Response Due to Team Organization	I-08: "Perhaps due to our team's context, which is well integrated into all processes, it was very easy to respond."

In summary, the general evaluation highlights the significant strengths of the LGPD-

Check project, particularly in its organization and conceptual clarity, as noted by the participants. The practical application of the recommendations and templates was praised, emphasizing their relevance and utility in ensuring compliance with LGPD requirements. Additionally, the interest demonstrated by external stakeholders, such as clients, reinforces the practical value and potential impact of the proposed approach. However, a suggestion was made to include references or links for each checklist item, which could further enhance the usability and traceability of the framework. These insights collectively validate the project's approach while offering constructive feedback for refinement and future iterations.

4.2.5 Implications of Results

The analysis conducted using LGPD-Check has yielded substantial insights into the compliance status of the *Coleta* and *Mercado Solidário* systems with LGPD requirements. The tool identified that 57.4% of the evaluated items exhibited non-conformities with legal standards, indicating significant gaps in data protection processes and practices. These findings provide a diagnostic of the current state of compliance and highlight areas that require attention and improvement to meet regulatory demands.

These results directly address the research questions by indicating LGPD-Check's capability to assess system compliance and identify areas of non-conformity. The findings support the tool's diagnostic utility, offering empirical evidence of its effectiveness in evaluating adherence to LGPD requirements. Furthermore, the analysis underscores its value in promoting a structured approach to data protection within organizational systems.

The high percentage of non-conformities identified raises important questions about the challenges of implementing LGPD in both legacy and developing systems. This observation suggests that even in institutions with technological resources, there remains a considerable path to achieving full compliance with data protection legislation. It highlights the necessity of incorporating "privacy by design" principles from the early stages of software development, an aspect that LGPD-Check can help promote.

The positive evaluation by participants regarding the clarity and usefulness of LGPD-Check's recommendations and templates indicates that the tool not only identifies issues but also offers practical solutions. This aspect is crucial for the effective adoption of the tool, as it facilitates the transition from identifying non-conformities to implementing corrections. The tool's ability to provide actionable insights can significantly reduce the time and resources required for organizations to achieve compliance.

Feedback from participants about the need to clearly distinguish between public and private data points to an area of potential improvement in the framework. This distinction is particularly relevant in the context of public institutions like UFMS, where the transparency of certain data needs to be balanced with the protection of individual privacy. Future developments of LGPD-Check could include specific guidance on how to navigate this delicate balance, potentially expanding its applicability across various organizational contexts.

The initial difficulty reported by participants in analyzing the checklist items emphasizes the importance of continuous training and familiarization with LGPD requirements. This suggests that LGPD-Check could be complemented with a capacity-building program, helping to build an organizational culture of data protection. Such an approach could extend the tool's impact beyond mere compliance, fostering a deeper understanding of data protection principles among users.

The suggestion to include references or links for each checklist item points to an opportunity to enrich the tool with educational resources. This would not only facilitate understanding and implementation of requirements but could also serve as a platform for continuous learning about best practices in data protection. By integrating educational components, LGPD-Check could evolve into a comprehensive resource for organizations seeking to improve their data governance practices.

From a broader perspective, the results have important implications for organizations aiming to comply with LGPD. They highlight the necessity of systematic and comprehensive evaluations to identify and address legal gaps in data protection. The findings underline the importance of adopting tools like LGPD-Check to guide compliance efforts. By identifying non-conformities and prioritizing corrective actions, organizations can allocate resources effectively to enhance their data protection frameworks, ensuring regulatory adherence and building trust with stakeholders.

Moreover, the study's outcomes suggest that LGPD-Check could serve as a model for other public organizations seeking to enhance their compliance with data protection laws. Its structured approach not only facilitates the identification of critical non-conformities but also provides a road-map for continuous improvement in data protection practices.

In conclusion, LGPD-Check has revealed its potential as a strategic asset in promoting compliance and continuous improvement in data protection practices. Its structured approach facilitates the identification of critical non-conformities and provides actionable insights for corrective measures. Beyond compliance, the tool supports organizations in strengthening their data governance practices, fostering a culture of accountability, and enhancing the security and trustworthiness of personal data handling. These implications underscore the value of LGPD-Check as a comprehensive solution for organizations navigating the complex landscape of data protection regulation.

4.3 Final Considerations

The focus group results emphasize the importance of clarity and support when addressing issues related to LGPD compliance. The initial difficulty in analyzing the checklist items highlights the need for consistent project updates and continuous familiarization with LGPD requirements. Clear and straightforward questions, alongside the usefulness of the recommendations, are pivotal to the effectiveness of the LGPD-Check framework. Consequently, it is advisable to regularly review and simplify the questions wherever possible and incorporate practical examples and guidelines to enhance user comprehension and application.

A clear distinction between public and private data must also be established to prevent misunderstandings. Additionally, quantifying the criticality of each question could provide a more structured assessment of the recommendations' impact, enabling a more targeted approach to compliance. Supplementary references, links, or resources for each checklist item were also suggested, which could further facilitate understanding and streamline the implementation of LGPD requirements.

To facilitate the reproducibility of this study, all related artifacts, which are available in Portuguese, have been made available in a package at Neitzke, Teixeira e Viana (2025). These improvements are not only expected to enhance the overall effectiveness of the LGPD-Check framework but also to contribute to sustained and efficient compliance with LGPD mandates. By providing a foundation for personal data protection and ensuring accountability on the part of data controllers, LGPD-Check can support organizations in fostering trust and adhering to their legal obligations while promoting best practices in data governance.

5 Conclusion

This master's thesis aimed to enhance the compliance of software systems with the LGPD, focusing mainly on systems used in Brazilian governmental organizations. The research began by advancing the LGPD-Check checklist, initially developed by Mendes, Viana e Rivero (2021), by incorporating new items derived from audit checklists used by TCU in federal public agencies. This updated version underwent a practical evaluation within a real-world environment at the TRE-MA, a public institution within the Brazilian Federal Judiciary.

The findings from the study conducted at TRE-MA enabled significant improvements to LGPD-Check. Beyond updating and refining the items and recommendations, we developed specific templates to support inspectors in using the checklist in practice. These templates empower LGPD-Check users to address and resolve non-compliance issues identified during inspections by providing standardized and actionable solutions.

To further assess the effectiveness of these enhancements, we conducted a second study involving participants from the Federal University of UFMS. In this study, two software systems under development by UFMS students were evaluated using LGPD-Check and its associated templates. After applying the checklist, participants engaged in a focus group to qualitatively assess the newly introduced recommendations and templates. The focus group results emphasized the templates' critical role in facilitating the resolution of non-compliance issues. Their inclusion not only enhances the efficiency of LGPD-Check but also strengthens its applicability in both academic settings and governmental institutions.

This research work concludes that integrating templates and continuously improving LGPD-Check are effective strategies for promoting greater adherence to the LGPD. This research's contributions extend beyond enhancing compliance in software systems, offering a practical and systematic approach to meeting the requirements of auditing and regulatory bodies.

Ultimately, we hope that the knowledge produced and the tools developed in this study serve as valuable references for professionals and researchers interested in adapting legal texts, laws, and regulations to the context of software systems. By bridging legal and technological perspectives, this work highlights the importance of interdisciplinary approaches in developing compliant and secure systems, addressing the growing demands for privacy and data protection in the digital age.

5.1 Contributions

This master's thesis presents several significant contributions, including:

- **Enhancement of the LGPD-Check software inspection checklist**: we improved the checklist to assess compliance with the LGPD, incorporating verification items based on quality attributes required by the LGPD, including items adapted from questionnaires used by the TCU to enhance its applicability in the context of public institutions.

- **Development of a set of templates**: For each item in the LGPD-Check, we designed templates to assist in implementing solutions to address non-compliance issues.

- **Definition of exploratory studies**: we outlined case studies to evaluate the feasibility of the inspection checklist and associated templates. These studies provide a replicable model for similar research objectives in the field.

- **Collaboration with TRE-MA and UFMS**: We practically applied the checklist in real-world systems from these governmental organizations, indicating its feasibility and effectiveness in an industrial context.

- **Addressing gaps in privacy and data protection within public institutions**: By focusing on compliance with the LGPD during system development, this work enhances privacy and protection practices in public sector systems.

- **Academic dissemination**:

  - Publication of the article *"Enhancing LGPD Compliance: Evaluating a Checklist for LGPD Quality Attributes within a Government Office"* in the proceedings of the XXII Brazilian Symposium on Software Quality (SBQS 2023), held in Brasília, DF, Brazil (NEITZKE et al., 2023).

  - Full citation:

    NEITZKE, C.; MENDES, J. A.; RIVERO, L.; TEIXEIRA, M.; VIANA, D. *Enhancing LGPD Compliance: Evaluating a Checklist for LGPD Quality Attributes within a Government Office.* In: *Proceedings of the XXII Brazilian Symposium on Software Quality.* New York, NY, USA: Association for Computing Machinery, 2023. (SBQS' 23), pp. 218–227. ISBN: 9798400707865. Available at: <https://doi.org/10.1145/3629479.3629497>.

  - **Submission of a second article**: An additional article has been submitted and is under review at the time of this thesis's publication.

These contributions reflect the advancements in bridging the gap between legal requirements and software development practices. They provide practical tools and methodologies for enhancing LGPD compliance in academic and governmental contexts.

5.2 Limitations and Threats to Validity

Despite this study's positive results, it is essential to acknowledge its limitations and threats to validity to ensure a critical analysis of the findings and contributions. As detailed below, the identified threats have been categorized into internal, external, conclusion, and construct validity.

Regarding **internal validity**, in addition to the author's direct involvement in the case study conducted at TRE-MA, which represents a potential source of bias, it should be noted that the templates themselves were created exclusively by the author. Although the author is an IT professional with knowledge of LGPD, the solitary development of the templates occurred due to time limitations available for research within the scope of a master's program. The unavailability of other experts for collaboration also contributed to the decision for individual creation. This circumstance may have limited the diversity of perspectives and experiences incorporated into the templates, potentially reducing their comprehensiveness or applicability in certain contexts. To mitigate this threat, we sought to validate the templates through evaluations with external participants in the second study conducted at UFMS, thus favoring a more impartial assessment of the developed artifacts.

Concerning **external validity**, the generalization of results is limited by the scope of the studies performed. We conducted evaluations in two contexts: TRE-MA, a federal judiciary body, and UFMS, a public academic institution. While these scenarios are representative, they may not fully capture the challenges faced in other domains, such as private organizations or multinational companies. Additionally, we refined the checklist focusing on LGPD compliance within Brazilian public institutions, which restricts its applicability to other privacy regulations, such as the European GDPR. Another significant factor is the technological dependency of LGPD-Check, which is currently implemented using Google Sheets and Google App Scripts. This dependency may limit adoption in organizations with restrictive policies regarding cloud-based tools or those requiring customized solutions.

Regarding the robustness of the evidence obtained, some limitations are related to **conclusion validity**. While we qualitatively evaluated the templates through focus group discussions, their effectiveness in more complex or large-scale scenarios remains untested. Furthermore, external factors, such as differences in the participants' technical knowledge levels, may have impacted the reliability of the conclusions drawn from the collected data.

Concerning **construct validity**, the effectiveness of the templates in addressing practical non-compliance issues may vary depending on the environment and the characteristics of the systems analyzed. Variations in requirements, organizational processes, and maturity levels in LGPD compliance across institutions may influence the success of the recommendations provided by the templates.

These limitations highlight the need for future studies to explore the generalization of results and the application of the framework in diverse domains and regulatory contexts. Despite these constraints, this research's contributions represent significant advancements in promoting LGPD compliance in software systems, particularly within the public sector.

The following section will present future perspectives on mitigating validity threats, including expanding application contexts and developing a customized software solution to enhance LGPD-Check's portability, efficiency, and usability.

5.3 Future Perspectives

The current version of LGPD-Check relies on Google Sheets technology integrated with Google App Scripts. However, several promising avenues for future development have been identified to enhance its functionality, applicability, and user experience. A key area for improvement involves the development of dedicated support software to enhance usability during the data collection and processing phases. This solution aims to streamline the workflow and improve user experience, making the checklist more accessible and efficient for its users.

Additionally, adapting the LGPD-Check framework to contexts beyond Brazil, such as the European GDPR, is considered a vital step for expansion. This adaptation would allow for exploring necessary modifications and extensions for GDPR compliance, thus broadening the framework's applicability and increasing its international relevance.

In the context of study replication, a crucial area for future enhancement has been identified: the introduction of a diary system during the use of LGPD-Check. This system would enable inspectors to record real-time suggestions for changes, difficulties encountered, and insights gained while using the tool. Such a mechanism could offer benefits, including the capture of immediate reactions, identification of specific use-case challenges, generation of quantitative data, and facilitation of continuous improvement. Importantly, this approach would enhance the traceability of improvement suggestions, allowing researchers to link specific recommendations to the context in which they were made and the exact items or features of LGPD-Check that prompted them. By allowing inspectors to document their experiences over time, this method could provide detailed data on user experience in various scenarios.

An exciting prospect for future development is the implementation of LGPD-related checks directly into the source code production pipeline. This integration would automate compliance verification during the development process, enabling real-time identification of potential privacy violations. By embedding data protection practices directly into the developers' workflow, it aims to foster a stronger "privacy by design" culture, reduce rework, and enhance overall code quality with respect to data protection.

Another innovative approach involves leveraging Generative AI to transform the checklist's results into comprehensive textual reports for organizations. This would automate the creation of reports from checklist data, generating clear and understandable documentation for non-technical stakeholders. By facilitating the communication of results and recommendations, this feature could improve the interpretation of collected data and support data-driven decision-making in compliance matters.

To validate and refine the framework, a new study is planned to apply the LGPD-Check in an external project without direct involvement from the checklist's authors. This study will evaluate the framework's effectiveness and acceptance by professionals working on real projects within the Information Technology Superintendency of UFMA. Positive results would support promoting LGPD-Check as a recommended technique for privacy protection in software system artifacts. Conversely, any identified shortcomings will inform further refinements to improve the technique's efficacy and reliability.

These future perspectives collectively present a commitment to enhancing LGPD-Check's capabilities, making it an increasingly valuable tool at the intersection of software development, data protection, and regulatory compliance. By addressing various aspects such as usability, international applicability, integration with development processes, automated reporting, and real-world validation, these proposed developments aim to advance the utility and impact of LGPD-Check in the field of data protection.

Bibliography

ALMEIDA, W. G. d. *Implementação de compliance à LGPD em instituições federais de ensino superior: proposta de um processo estruturado para conformidade.* Dissertação (Mestrado) — Universidade Federal de São Carlos, 2024. Quoted on page 27.

ARAUJO, E.; VILELA, J.; SILVA, C.; ALVES, C. Are my business process models compliant with lgpd? the lgpd4bp method to evaluate and to model lgpd aware business processes. In: *XVII Brazilian Symposium on Information Systems*. New York, NY, USA: Association for Computing Machinery, 2021. (SBSI 2021), p. 1–9. ISBN 9781450384919. Disponível em: <https://doi.org/10.1145/3466933.3466982>. Quoted on page 26.

BARATI, M.; AUJLA, G. S.; LLANOS, J. T.; DUODU, K. A.; RANA, O. F.; CARR, M.; RAJAN, R. Privacy-aware cloud auditing for gdpr compliance verification in online healthcare. *IEEE Transactions on Industrial Informatics*, IEEE, 2021. Quoted on page 26.

BASILI, V. R.; ROMBACH, H. D. The tame project: Towards improvement-oriented software environments. *IEEE Transactions on software engineering*, IEEE, v. 14, n. 6, p. 758–773, 1988. Quoted on page 33.

BASTOS, A.; RIOS, E.; CRISTALLI, R.; MOREIRA, T. et al. Base de conhecimento em teste de software. *São Paulo*, v. 30, p. 32, 2007. Quoted on page 32.

BECKER, R.; ALPER, P.; GROUÈS, V.; MUNOZ, S.; JAROSZ, Y.; LEBIODA, J.; REGE, K.; TREFOIS, C.; SATAGOPAM, V.; SCHNEIDER, R. Daisy: A data information system for accountability under the general data protection regulation. *GigaScience*, Oxford University Press, v. 8, n. 12, p. giz140, 2019. Quoted on page 25.

BRASIL. *Lei N° 13.709, de 14 De Agosto De 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)*. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Quoted 6 times on page(s) 14, 21, 22, 23, 24, and 30.

BRAZIL. *Constitution of the Federative Republic of Brazil*. Presidência da República, 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>. Quoted on page 33.

BRAZIL. *Supplementary Law No. 75 of 1993: Article 76*. Presidência da República, 1993. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp75.htm#art76>. Quoted on page 33.

CAMÊLO, M. N.; ALVES, C. G-priv: Um guia para apoiar a especificação de requisitos de privacidade em conformidade com a lgpd. *iSys-Brazilian Journal of Information Systems*, v. 16, n. 1, p. 2–1, 2023. Quoted on page 27.

CANEDO, E. D.; CALAZANS, A. T. S.; BANDEIRA, I. N.; COSTA, P. H. T.; MASSON, E. T. S. Guidelines adopted by agile teams in privacy requirements elicitation after the brazilian general data protection law (lgpd) implementation. *Requirements Engineering*, Springer, v. 27, n. 4, p. 545–567, 2022. Quoted 2 times on page(s) 26 and 27.

CANEDO, E. D.; CALAZANS, A. T. S.; CERQUEIRA, A. J.; COSTA, P. H. T.; MASSON, E. T. S. Agile teams' perception in privacy requirements elicitation: Lgpd's compliance in brazil. In: IEEE. *2021 IEEE 29th International Requirements Engineering Conference (RE)*. [S.l.], 2021. p. 58–69. Quoted 3 times on page(s) 15, 16, and 27.

CANEDO, E. D.; CALAZANS, A. T. S.; MASSON, E. T. S.; COSTA, P. H. T.; LIMA, F. Perceptions of ict practitioners regarding software privacy. *Entropy*, v. 22, n. 4, 2020. ISSN 1099-4300. Disponível em: <https://www.mdpi.com/1099-4300/22/4/429>. Quoted on page 25.

CAVOUKIAN, A. et al. Privacy by design: The seven foundational principles. *IAPP Resource Center, https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles*, 2021. Quoted on page 20.

CELIDONIO, T.; NEVES, P. S.; DONÁ, C. M. 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/methodology for mapping and adequacy of the requirements listed in lgpd (brazil data protection general law number 13 709/18) in a financial institution-a case study. *Brazilian Journal of Business*, v. 2, n. 4, p. 3626–3648, 2020. Quoted on page 26.

CERQUEIRA, D. A. *LGPDCHECK: INSPEÇÃO DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS EM ARTEFATOS DE SOFTWARE À LUZ DOS PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD-13.709/2018)*. Tese (Doutorado) — Universidade Federal do Rio de Janeiro, 2024. Quoted on page 27.

DALL'AGNOL, C. M.; TRENCH, M. H. Grupos focais como estratégia metodológica em pesquisas na enfermagem. *Revista gaúcha de enfermagem. Porto Alegre. Vol. 20, n. 1 (jan. 1999), p. 5-25*, 1999. Quoted 2 times on page(s) 37 and 51.

DAVIS, F. D.; BAGOZZI, R. P.; WARSHAW, P. R. User acceptance of computer technology: A comparison of two theoretical models. *Management science*, INFORMS, v. 35, n. 8, p. 982–1003, 1989. Quoted 3 times on page(s) 34, 36, and 37.

DEBUS, M. Manual para excelencia en la investigación mediante grupos focales. In: *Manual para excelencia en la investigación mediante grupos focales*. [S.l.: s.n.], 1994. p. 97–97. Quoted on page 36.

DUARTE, T. X. D. et al. *Tecnologia, uso, coleta e tratamento de dados: o futuro do poder econômico?* Dissertação (Mestrado) — Universidade Nove de Julho, 2020. Quoted on page 14.

European Commission. *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) (Text with EEA relevance)*. European Commission, 2016. Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Quoted 2 times on page(s) 14 and 30.

FAGAN, M. E. Design and code inspections to reduce errors in program development. *IBM Syst. J.*, v. 38, p. 258–287, 1976. Disponível em: <https://api.semanticscholar.org/CorpusID:8930121>. Quoted on page 24.

FERRÃO, S. É. R.; CARVALHO, A. P.; CANEDO, E. D.; MOTA, A. P. B.; COSTA, P. H. T.; CERQUEIRA, A. J. Diagnostic of data processing by brazilian organizations—a low compliance issue. *Information*, Multidisciplinary Digital Publishing Institute, v. 12, n. 4, p. 168, 2021. Quoted 3 times on page(s) 15, 16, and 27.

GÜRSES, S.; TRONCOSO, C.; DIAZ, C. Engineering privacy by design reloaded. In: *Amsterdam Privacy Conference*. [S.l.: s.n.], 2015. v. 21, p. 1–21. Quoted 2 times on page(s) 21 and 22.

IEEE. Ieee standard for software reviews and audits. *IEEE Std 1028-2008*, p. 1–53, Aug 2008. Quoted on page 24.

KALINOWSKI, M.; SPÍNOLA, R. O.; TRAVASSOS, G. H. Infra-estrutura computacional para apoio ao processo de inspeção de software. *III Simpósio Brasileiro de Qualidade de Software, Brasília, Brasil*, p. 62–77, 2004. Quoted 2 times on page(s) 17 and 24.

KONTIO, J.; LEHTOLA, L.; BRAGGE, J. Using the focus group method in software engineering: obtaining practitioner and user experiences. In: IEEE. *Proceedings. 2004 International Symposium on Empirical Software Engineering, 2004. ISESE'04.* [S.l.], 2004. p. 271–280. Quoted on page 36.

KUBICEK, K.; MERANE, J.; COTRINI, C.; STREMITZER, A.; BECHTOLD, S.; BASIN, D. Checking websites' gdpr consent compliance for marketing emails. *Proceedings on Privacy Enhancing Technologies*, Proceedings on Privacy Enhancing Technologies, 2022. Quoted on page 26.

LAITENBERGER, O.; EMAM, K. E.; HARBICH, T. An internally replicated quasi-experimental comparison of checklist and perspective based reading of code documents. *IEEE Transactions on Software Engineering*, v. 27, n. 5, p. 387–421, 2001. Quoted 2 times on page(s) 24 and 31.

LORENZON, L. N. Análise comparada entre regulamentações de dados pessoais no brasil e na união europeia (lgpd e gdpr) e seus respectivos instrumentos de enforcement. *Revista do Programa de Direito da União Europeia*, v. 1, p. 39–52, 2021. Quoted on page 14.

MACHADO, R.; KREUTZ, D.; PAZ, G.; RODRIGUES, G. Vazamentos de dados: Histórico, impacto socioeconômico e as novas leis de proteçao de dados. In: SBC. *Anais da XVII Escola Regional de Redes de Computadores.* [S.l.], 2019. p. 154–159. Quoted on page 14.

MAZZA, V. de A.; MELO, N. S. F. de O.; CHIESA, A. M. O grupo focal como técnica de coleta de dados na pesquisa qualitativa: relato de experiência. *Cogitare Enfermagem*, v. 14, n. 1, 2009. Quoted 2 times on page(s) 37 and 50.

MCIVER, J.; CARMINES, E. G. *Unidimensional scaling.* [S.l.]: Sage, 1981. v. 24. Quoted on page 36.

MELLO, R.; MASSOLLAR, J.; TRAVASSOS, G. Técnica de inspeção baseada em checklist para identificação de defeitos em diagramas de atividades. In: *Anais do X Simpósio Brasileiro de Qualidade de Software.* Porto Alegre, RS, Brasil: SBC, 2011. p. 119–133. ISSN 0000-0000. Disponível em: <https://sol.sbc.org.br/index.php/sbqs/article/view/15391>. Quoted on page 24.

MENDES, J.; VIANA, D.; RIVERO, L. Developing an inspection checklist for the adequacy assessment of software systems to quality attributes of the brazilian general data protection law: An initial proposal. In: *Brazilian Symposium on Software Engineering.* [S.l.: s.n.], 2021. p. 263–268. Quoted 9 times on page(s) 17, 18, 25, 29, 30, 31, 33, 44, and 60.

MORTE, A. B.; MEIRA, A.; COSTA, R.; MARIZ, D. Uma análise sobre o uso de dlts no tratamento de dados pessoais: Aderência aos princípios e direitos elencados na lgpd. In: *Anais do III Workshop em Blockchain: Teoria, Tecnologia e Aplicações.* Porto Alegre, RS, Brasil: SBC, 2020. p. 74–87. ISSN 0000-0000. Disponível em: <https://sol.sbc.org.br/index.php/wblockchain/article/view/12435>. Quoted on page 26.

NEITZKE, C.; MENDES, J. a.; RIVERO, L.; TEIXEIRA, M.; VIANA, D. Enhancing lgpd compliance: Evaluating a checklist for lgpd quality attributes within a government office. In: *Proceedings of the XXII Brazilian Symposium on Software Quality.* New York, NY, USA:

Association for Computing Machinery, 2023. (SBQS ’23), p. 218–227. ISBN 9798400707865. Disponível em: <https://doi.org/10.1145/3629479.3629497>. Quoted 5 times on page(s) 33, 34, 35, 44, and 61.

NEITZKE, C. A.; TEIXEIRA, M. M.; VIANA, D. *Reproducibility Package for: Enhancing LGPD Compliance – A Specialized Checklist and Implementation Templates for Governmental Software Systems*. Zenodo, 2025. Disponível em: <https://doi.org/10.5281/zenodo.14984879>. Quoted on page 59.

NETO, I. P. G.; MENDES, J.; FERREIRA, W.; RIVERO, L.; VIANA, D.; SOARES, S. An lgpd compliance inspection checklist to assess iot solutions. In: *Companion Proceedings of the 32nd ACM International Conference on the Foundations of Software Engineering*. [S.l.: s.n.], 2024. p. 340–350. Quoted on page 25.

NIELSEN, J. Usability inspection methods. In: *Conference companion on Human factors in computing systems*. [S.l.: s.n.], 1994. p. 413–414. Quoted on page 32.

PEIXOTO, M.; FERREIRA, D.; CAVALCANTI, M.; SILVA, C.; VILELA, J.; ARAúJO, J.; GORSCHEK, T. On understanding how developers perceive and interpret privacy requirements research preview. In: MADHAVJI, N.; PASQUALE, L.; FERRARI, A.; GNESI, S. (Ed.). *Requirements Engineering: Foundation for Software Quality*. Cham: Springer International Publishing, 2020. p. 116–123. ISBN 978-3-030-44429-7. Quoted on page 25.

PELOSO, F.; COSTA, M. A.; FROGERI, R. F.; CALEGARIO, C. L. L. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. *Suma de Negocios*, v. 10, n. 23, p. 89–99, 2019. Quoted on page 15.

RINGMANN, S. D.; LANGWEG, H.; WALDVOGEL, M. Requirements for legally compliant software based on the gdpr. In: *Cloud and Trusted Computing 2018 (CeTC 2018)*. [s.n.], 2018. p. 1–18. Disponível em: <https://netfuture.ch/wp-content/uploads/2018/10/ringmann2018requirements.pdf>. Quoted 3 times on page(s) 14, 17, and 29.

ROJAS, M. A. T. *Avaliação da adequação do Instituto Federal de Santa Catarina á Lei Geral de Proteção de Dados Pessoais*. 2020. Quoted on page 26.

SAUER, C.; JEFFERY, D. R.; LAND, L.; YETTON, P. The effectiveness of software development technical reviews: A behaviorally motivated program of research. *IEEE Transactions on Software Engineering*, IEEE, v. 26, n. 1, p. 1–14, 2000. Quoted on page 33.

SHAPIRO, S. S. Privacy by design: moving from art to practice. *Commun. ACM*, Association for Computing Machinery, New York, NY, USA, v. 53, n. 6, p. 27–29, jun. 2010. ISSN 0001-0782. Disponível em: <https://doi.org/10.1145/1743546.1743559>. Quoted on page 15.

SHULL, F.; TRAVASSOS, G. H.; CARVER, J.; BASILI, V. R. *Evolving a set of techniques for OO inspections*. [S.l.]: Digital Repository at the University of Maryland, 1999. Quoted on page 24.

SOUZA, J. S.; ABE, J. M.; LIMA, L. A. de; SOUZA, N. A. de. The general law principles for protection the personal data and their importance. *arXiv preprint arXiv:2009.14313*, 2020. Quoted on page 14.

Tribunal de Contas da União. *Diagnóstico sobre os controles implementados pelas organizações públicas federais para adequação à LGPD*. [S.l.]: Tribunal de Contas da União, 2022. Diagnóstico sobre os controles implementados pelas organizações públicas federais para adequação à LGPD. Quoted 4 times on page(s) 15, 16, 18, and 30.

Appendices

A Informed Consent Form

Dear Participant,

The Graduate Program in Computer Science (PPGCC) at the Federal University of Maranhão occasionally conducts experimental studies aimed at characterizing and evaluating different software technologies. You have been previously selected based on your profile, knowledge, and experience, and we are now inviting you to participate in this research. Data collection for this study will be conducted through a practical assignment. It is important to emphasize that, even though the practical assignment is part of the research, you have the right to refuse the use of your assignment data for research purposes.

1) Procedures

The study will be conducted individually, following the protocol established by the responsible researcher. At the end of the study, participants will be asked to complete an evaluation questionnaire regarding the software technology under analysis, as well as to participate in a focus group interview.

2) Handling of Potential Risks and Discomforts

All necessary measures will be taken during data collection to ensure participants' privacy and anonymity.

3) Benefits and Costs

This study is expected to enhance your knowledge, contributing to improving the quality of the activities in which you are involved or may engage in the future. Additionally, the results obtained will be of great importance to research in the PPGCC. It is emphasized that your participation in the study will not incur any expense or burden, and no reimbursement or compensation will be provided as a result of authorizing the use of your data for research purposes.

4) Research Confidentiality

All information collected in this study is confidential, and your name will not be identified in any way unless explicit authorization is granted for this purpose. During data collection, your name will be anonymized and will not be used at any stage of the analysis or presentation of results.

5) Participation

We appreciate your participation in this study, which is voluntary and of great importance. Your free and informed consent is required for the use of the data collected. You have the right to choose not to participate or to withdraw from the study at any time without any penalties. If you decide to withdraw, please notify the responsible researcher.

6) Declaration of Free and Informed Consent

I declare that I have carefully read and agree with the information presented in this document. The technical language used in the description of this research study was adequately explained, and all my doubts were clarified. I understand that I have the right to refuse the use of my data in this study at any time, without suffering any penalty. I confirm that I am over 18 years of age and voluntarily agree to participate in this study.

[ ] Yes [ ] No ____

B Participant Characterization Form

Full Name: ____

Age: ____________

Gender:

[ ] Male [ ] Female [ ] Other: ______________________

Education Level:

[ ] High School [ ] Undergraduate [ ] Postgraduate [ ] Master's Degree [ ] Doctorate

Current Position: ____

Years of Experience in Current Position: ____________

Do you have knowledge of software inspection?

[ ] Yes [ ] No

Do you have knowledge of the Brazilian General Data Protection Law (LGPD)?

[ ] Yes [ ] No

Briefly describe your knowledge about the LGPD:

____

____

____

____

____

C Assessment Questionnaire

This form is used to evaluate the compliance of the LGPD-Check in terms of usability, usefulness, and intention to use. Please indicate your level of agreement with the following statements based on your perception after using the checklist.

Legend:

Strongly Agree (SA), Somewhat Agree (SWA), Somewhat Disagree (SWD) and Strongly Disagree (SD).

Usability:

Statement	**SA**	**SWA**	**SWD**	**SD**
The checklist was clear and easy to understand.	[ ]	[ ]	[ ]	[ ]
Overall, I find it easy to detect defects or issues in a system using the checklist.	[ ]	[ ]	[ ]	[ ]
The checklist required little mental effort.	[ ]	[ ]	[ ]	[ ]

Usefulness:

Statement	**SA**	**SWA**	**SWD**	**SD**
The checklist allows me to inspect the system more quickly.	[ ]	[ ]	[ ]	[ ]
The checklist improves my productivity when identifying defects or issues in the system.	[ ]	[ ]	[ ]	[ ]
I believe the checklist is useful for detecting defects or issues in the system.	[ ]	[ ]	[ ]	[ ]

Intention to Use:

Statement	**SA**	**SWA**	**SWD**	**SD**
I intend to use the checklist to detect defects or issues in the system in the future.	[ ]	[ ]	[ ]	[ ]
I would recommend the checklist to other development teams.	[ ]	[ ]	[ ]	[ ]

Comments:

____

____

____

____

____

D LGPD-Check

D.1 General Instructions

This checklist aims to evaluate systems' compliance with the General Data Protection Law (LGPD). The list contains 61 items, divided into two parts: 47 mandatory items, required by the LGPD, and 14 optional items, which are beneficial suggestions and improvement opportunities. The items are organized into five categories: Data Transparency, User Consent, User Rights, Data Security, and Controller Responsibilities.

Item Evaluation

The evaluator must indicate in the "Response" column whether the item is:

1 - Yes (adequate and compliant)

2 - No (defective or inadequate)

3 - Not applicable (when the item is not relevant to the type of data processing carried out by the institution)

Severity Level

For items considered inadequate or defective, the evaluator must mark the severity level of the failure in the "Severity Level" column:

1 - Minor

2 - Major

3 - Catastrophic

Evaluator's Comments

This column is optional and allows the evaluator to record any observations, suggestions, questions, identified issues, problem locations, clarifications about the evaluation, etc.

Recommendations

This section is intended for optional comments and suggestions on how to better adapt the item to the LGPD requirements.

Templates

This section contains a link to more detailed suggestions on how to address potential non-compliance issues.

Summary

The "Summary" tab contains general checklist data and two monitoring charts:

- **Progress Chart:** Displays the percentage of the table's completion.
- **Compliance Index Chart:** Shows the compliance rate of the items, the failure rate, the non-applicable item rate, and the unfilled item rate.

Glossary

For additional terminology and definitions, visit:

`https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/glossario-anpd`

Category Summary

Code	**Category**	**Number of Items**
T	Data Transparency	14
C	User Consent	8
D	User Rights	15
S	Data Security	17
R	Controller Responsibility	7

Item Classification

Description	**Number of Items**
Mandatory Items	47
Optional Items	14

Evaluation Details

Evaluator's Name:	
Systems Evaluated:	
Workplace:	
Inspection Start Date:	
Inspection End Date:	
Minutes Spent Completing:	

D.2 Check-list

ID	**Mand.**	**Item Assessed**
T-01	Yes	Has the organization defined the purposes of data processing?
T-02	Yes	Is personal data processing carried out according to a legal basis?

T-03	Yes	Does the system inform the data subject about the purposes of personal data processing?
T-04	Yes	Does the system process personal data in compliance with the purpose presented to the data subject?
T-05	Yes	Does the system inform the data subject about the method and duration of personal data processing in a free and accessible manner?
T-06	Yes	Does the system allow the data subject to access their personal data in full, free of charge, and in an accessible manner?
T-07	Yes	Does the system accurately and clearly store personal data collected from data subjects?
T-08	Yes	Does the system keep personal data updated as necessary to fulfill the purpose of its processing?
T-09	Yes	Does the system provide the data subject with information about data processing and the controller's identity?
T-10	Yes	Does the organization process data based on legitimate interest in accordance with the law?
T-11	Yes	Does the system keep records of data processing operations, especially when based on legitimate interest?
T-12	Yes	Does the system inform the data subject and competent authorities about data processing operations, especially when based on legitimate interest?
T-13	Yes	Does the system process personal or sensitive data in a way that prevents it from being connected to a data subject when requested?
T-14	Yes	Does the system inform the data subject about data processing before collection?
C-01	Yes	Does the system allow the data subject to provide consent clearly and autonomously for data processing?
C-02	Yes	Does the system request specific consent from the data subject to communicate or share personal data with other controllers?
C-03	Yes	Does the system store the data subject's consent for legal proof?
C-04	Yes	Does the system allow the data subject to refuse or withdraw consent without any penalties?
C-05	Yes	Does the system process personal data of children and adolescents only with specific consent from parents or legal guardians, in an accessible and understandable way?
C-06	Yes	Does the system inform the data subject about changes in purpose and consent updates, allowing withdrawal of consent if the data subject disagrees with changes?
C-07	Yes	Does the system provide a consent declaration in an understandable and easily accessible way, free from abusive terms?
C-08	Yes	Does the system inform the data subject about all their rights in the consent declaration?
D-01	Yes	Does the system store personal data in a format that facilitates access by the data subject?
D-02	Yes	Does the system provide the data subject with means to file complaints regarding data protection and processing?
D-03	Yes	Does the system provide the data subject with a full electronic copy of their personal data?
D-04	Yes	Does the system allow the data subject to update their personal data?
D-05	Yes	Does the system only use relevant and adequate data for the intended purpose?

D-06	Yes	Does the system allow data portability to another controller upon the data subject's request?
D-07	Yes	Does the system allow deletion of personal data upon the data subject's request?
D-08	Yes	Does the system delete the data subject's personal data after processing ends?
D-09	Yes	Does the system provide information about public and private entities involved in personal data sharing?
D-10	Yes	Does the system inform the data subject about the possibility of refusing consent and the consequences of refusal?
D-11	Yes	Does the system inform the data subject when data processing is a requirement for product provision, service delivery, or exercising rights?
D-12	Yes	Does the system allow the data subject to object to data processing easily?
D-13	Yes	Does the system inform the data subject about reasons for the delayed exercise of their rights?
D-14	Yes	Does the system inform the data subject when decisions are made based on automated data processing, including profiling?
D-15	Yes	Does the system provide the data subject with an option to challenge or request a review of automated decisions?
S-01	Yes	Does the system process data securely, including protection against unauthorized access?
S-02	Yes	Does the system comply with personal data transfer regulations to international countries with adequate protection?
S-03	Yes	Does the system inform the data subject about international data transfers?
S-04	Yes	Does the system use mechanisms to prevent data damage, destruction, or loss?
S-05	Yes	Does the system apply adequate protection measures for sensitive personal data?
S-06	No	Does the system adopt privacy best practices, such as privacy by design?
S-07	No	Does the system perform mapping of personal data and keep it secure?
S-08	No	Does the system ensure confidentiality by using appropriate technical measures?
S-09	No	Does the system ensure the integrity of personal data, preventing modifications?
S-10	No	Does the system maintain audit logs of compliance and provide information to the data subject upon request?
S-11	No	Does the organization have a privacy and security incident response plan?
S-12	No	Does the system have certifications or seals to demonstrate compliance with personal data protection standards?
S-13	No	Does the system implement a process for registration, cancellation, and provisioning for access control?
S-14	No	Does the system have a formal process for registering and canceling users of systems that handle personal data?
S-15	No	Does the system have a formal process for granting or revoking access rights?
S-16	No	Does the system maintain an accurate and up-to-date record of users authorized to access information systems or personal data contained within them?
S-17	No	Does the system implement the protection of personal data both in transit (SSL) and at rest?
R-01	Yes	Does the organization appoint a Data Protection Officer (DPO) responsible for data processing?

R-02	Yes	Does the organization publicly disclose the DPO's identity and contact details clearly and objectively?
R-03	Yes	Does the organization notify the national authority and the data subject in case of a security incident posing significant risks or damages?
R-04	Yes	Does the organization conduct a data protection impact assessment when data processing involves high risks to data subjects' rights and freedoms?
R-05	Yes	Does the organization prepare a data protection impact report and provide it to the national authority when requested?
R-06	No	Does the organization record the DPO's activities for legal proof?
R-07	No	Does the organization provide training to employees on LGPD compliance?

D.3 Recommendations

ID	**Recommendation**
T-01	Create a document defining a Privacy Policy and Consent Terms, describing the purposes of data processing and how the data will be used.
T-02	In the documentation of the Privacy Policy and Consent Terms, explain the legal basis that justifies the processing of personal data. Examples of legal bases include: I - Upon the provision of consent by the data subject; II - For the fulfillment of a legal or regulatory obligation by the data controller. For the complete list of legal bases, refer to Chapter 2, Section 1, Article 7 of the applicable data protection law.
T-03	The system must make the Privacy Policy and/or Consent Terms available to the data subject, detailing the purposes of the data processing.
T-04	Review the consent and implement changes that are not in compliance with what was communicated to the data subject.
T-05	In the Privacy Policy document and the Consent Terms, describe how the data processing will be carried out and its duration, ensuring this information is always made available to the data subject.
T-06	Create a communication channel between the data subject and the company to facilitate the data subject's ability to request the entirety of their personal data. This channel should always be free of charge and ensure efficient processing without delays.
T-07	During data collection, ensure that personal data is being provided accurately. For example, implement field validation in forms (e.g., for CPF, CEP, or other relevant data).
T-08	Create a process to map and review personal data in the database. If it is discovered that personal data is incorrect, it must be corrected or deleted as quickly as possible. Whenever necessary, request that the data subject update their data to ensure the fulfillment of the processing purposes.
T-09	Provide the data subject with clear and precise information in the Privacy Policy and Consent Terms about: a) Purposes of Processing; b) The identity and contact information of the data controller; c) The data involved; d) The legal basis; e) Details of data transfers outside Brazil; f) The data retention period; g) The data subject's rights.

T-10	The company will conduct a legitimate interest assessment to verify whether the processing hypothesis can be justified under this legal basis. This assessment must demonstrate that: a) There is a valid legitimate interest; b) The data processing is strictly necessary to pursue the legitimate interest; and c) The processing is not overridden by or harmful to the individual's rights.
T-11	Store in the database information about data processing operations for potential legal verification.
T-12	Prepare reports on data processing operations, especially when based on legitimate interest, and make them available when requested by the data subject or competent authorities, such as the ANPD.
T-13	Analyze which personal data should be anonymized or, in other cases, pseudonymized. Example: A version similar to the original data but without revealing the true information of the data subject.
T-14	Make it clear and prominent to the data subject, with notices, which personal data will be collected, and request the data subject's consent.
C-01	In the Consent Terms, it is recommended to use clear and objective language, avoid misleading advertising, refrain from using pre-checked boxes, and provide an option for the data subject to deny or withdraw their consent without any detriment.
C-02	It is mandatory to be transparent with the data subject about the purpose of processing their data. Especially when sharing data with other controllers, the data subject must be clearly informed in the consent form.
C-03	Store the data subject's consent records in the database for verification purposes.
C-04	The data subject must have access to their Consent Terms or contract with the option to deny the processing of their data.
C-05	It must be ensured that only the legitimate individual can provide consent, and only they can update it. An example is to authenticate the data subject.
C-06	Whenever there is a change in the purpose of processing, the data subject must be informed of the change and a new consent must be requested for data processing, with the option to deny processing if the data subject disagrees with the change.
C-07	The Consent Terms must be well-written, using easily understandable language, and respecting the rights of the data subject.
C-08	The Consent Terms and Privacy Policy must inform the data subjects of the rights they possess.
D-01	To facilitate access for data subjects, personal data should be stored in computer-readable formats, in structured files, so that software applications can easily identify, recognize, and extract the personal data. Some examples include: CSV, XML, and JSON.
D-02	Provide the contact information of the DPO (Data Protection Officer) or the person responsible for data processing in the Privacy Policy or on a dedicated page for complaints.
D-03	Transmit the requested data directly to the data subject; or provide access to a tool that allows the data subject to extract the requested data themselves.
D-04	Depending on the purpose of the processing, it is necessary to request updates to the data subject's personal data. It is recommended to create a mechanism that allows the data subject to update their personal data themselves.
D-05	It is necessary to minimize personal data, using only relevant data for processing. It is recommended to anonymize unnecessary data, and to block or delete irrelevant personal data.

D-06	Personal data should be stored in a machine-readable and accessible format, so that the data subject's information can be exported upon their request.
D-07	Create a mechanism to allow the data subject to request the removal of their personal data.
D-08	It is necessary to delete the data subject's personal data after the purpose has been fulfilled, within the established timeframe.
D-09	Store information about the entities and the processing operations carried out, such as data sharing, for legal verification purposes, and make it available when requested.
D-10	The Consent Form must provide the option to refuse processing, as well as the consequences if the data subject does not wish to consent.
D-11	The objectives and prerequisites of data processing must be clearly stated at the time of the data subject's consent.
D-12	It is necessary to provide a mechanism for the data subject to withdraw their consent. If consent is withdrawn, the data subject's information can no longer be processed.
D-13	When it is not possible to immediately fulfill a requested operation, a response must be sent to the data subject, which in some cases may: I - inform that the company is not the data processing agent and indicate, whenever possible, the responsible agent; or II - state the factual or legal reasons that prevent the immediate execution of the operation.
D-14	Provide the data subject with information about the automated decisions that will be made. If requested, supply the records of such information.
D-15	If requested, the contested automated decision must be reviewed, which may involve halting the data processing and obtaining new consent for that purpose.
S-01	Ensure the security of personal data processing by allowing only authorized individuals to read, modify, or delete data from the system. A recommended example would be to create an access control list.
S-02	Verify whether the destination country of the data transfer has a level of protection equal to or higher than that provided for under the LGPD and/or whether the recipient company can demonstrate that it offers the same guarantees of protection through standards or certifications. Also, confirm whether the ANPD authorizes such operations.
S-03	Include in the Privacy Policy document and the Consent Form information about the transfer of data to international countries.
S-04	It is necessary to create a mechanism to prevent the loss of and damage to the data subject's personal data. As best practices, implement data backup, cloud storage, and any other measures that will protect the original information in case of damage, destruction, or data loss.
S-05	It is necessary to implement an additional layer of security and storage, especially for sensitive personal data. Examples include, in some cases, using data encryption, access control, and other recommended techniques.
S-06	As a best practice for system development and compliance, implement the privacy by design methodology.
S-07	Organize the locations where data is collected and stored.
S-08	Ensure protection against unauthorized access when using stored or in-transit personal data. Examples include implementing authentication and access control.
S-09	Verify the integrity of data during collection and processing of personal data.
S-10	One solution would be to document the data from audits conducted to provide to the data subject.
S-11	The organization should document a plan for addressing security flaws or incidents.

S-12	It is recommended that systems have a certification that proves they follow a reliable code of conduct or security policy for adherence to data protection laws. Some examples include: ISO 27001, ISO 27701.
S-13	For effective access control, implement a secure registration system that can validate and store user information with unique credentials. Use hash functions and salting practices to enhance security. Additionally, create automated or semi-automated processes to remove users when they are no longer needed. The system should also manage access to resources by defining roles and permissions, assigning these roles to users, and applying role-based access control policies.
S-14	To control access to systems that handle personal data, implement a secure process for user registration and cancellation, with strong permission and password policies. Use auditing to track activities, conduct regular security training, and have a post-cancellation data deletion policy. Ensure that the software complies with data privacy regulations.
S-15	To address the issue of granting or revoking access rights in a system, it is suggested to implement an Identity and Access Management (IAM) system. This solution offers functionalities such as identity provisioning, multi-factor authentication, permission and role management, password management, access auditing and reporting, and deprovisioning. This allows for secure and efficient control over who has access to what within the system, increasing information security and operational efficiency.
S-16	Maintain a detailed record of all user activities. These include when and by whom a resource was accessed, modified, or deleted. This will help track suspicious activities and investigate security incidents.
S-17	SSL (Secure Sockets Layer) or its successor TLS (Transport Layer Security) are security protocols that help protect data integrity while it's being transmitted. Stored personal data can be encrypted to ensure that even if someone gains physical or remote access to the data, they still cannot read it. There are various strategies to do this, depending on the specific requirements of your system. For example, you can use disk-level encryption (such as BitLocker on Windows or FileVault on macOS), database-level encryption (such as Transparent Data Encryption in Oracle), or application-level encryption (for instance, using encryption libraries to encrypt data before storing it).
R-01	The organization must appoint a Data Protection Officer (DPO), who can be either an individual or a legal entity, to act as a communication channel between the controller, data subjects, and the ANPD. The ANPD may establish complementary rules regarding the DPO's activities, including exemption from their appointment, depending on the nature of the organization.
R-02	The information must be clearly stated in the Privacy Policy and the Consent Form, so that data subjects and the national authority can have easy access.
R-03	In the event of a security incident, it is necessary to notify the data subject and the ANPD. The recommended timeframe for notification by the ANPD is 2 business days from the awareness of the incident (even if it is not yet confirmed and under investigation). A preliminary notification should be sent, under penalty of violating the LGPD. The content of the notification must cover, at minimum, what is provided in §1 of art. 48 of the LGPD.
R-04	The organization must conduct a data protection impact assessment when there is a high risk in data processing. Ensure that the assessment is always reviewed, especially if the degree of risk in data processing is high.

R-05	It is necessary to prepare a data protection impact report and make it available when requested. The report should contain, at a minimum, a description of the types of data collected, the methodology used for collection and for ensuring information security, and the controller's analysis regarding measures, safeguards, and risk mitigation mechanisms adopted.
R-06	Store and document the history of activities of the appointed DPO.
R-07	Train employees and collaborators on the information that the LGPD determines. Examples: Through training sessions, courses, lectures, certifications, etc.

E Templates

E.1 Transparency Templates

T-01: Have the purposes of data processing been defined within the organization?

Privacy Policy Draft and Consent Terms

Introduction: This Privacy Policy aims to inform users how [Organization Name] collects, uses, shares, and protects the personal data provided. This policy complies with the General Data Protection Law (LGPD) and other applicable legislation.

1. Definitions: For the purposes of this Privacy Policy, the following definitions are adopted:

- **Personal Data:** Information related to an identified or identifiable natural person.
- **Data Subject:** The individual to whom the personal data refers.
- **Data Processing:** Any operation performed with personal data, such as collection, storage, use, sharing, among others.
- **Controller:** The individual or legal entity, of public or private law, responsible for decisions regarding the processing of personal data.
- **Processor:** The individual or legal entity, of public or private law, who processes personal data on behalf of the controller.

2. Legal Basis for Data Processing: [Organization Name] processes personal data based on the following legal bases, according to Article 7 of the LGPD:

1. **With the Consent of the Data Subject:** Processing is carried out with the free, informed, and unequivocal consent of the data subject. *Example: Sending newsletters, promotional communications.*
2. **For Compliance with Legal or Regulatory Obligations:** Data is used to comply with legal and regulatory obligations. *Example: Storage of tax and accounting data, audit purposes.*
3. **For Execution of Contracts or Pre-Contractual Measures:** Data necessary for the execution of contracts or related preliminary procedures. *Example: Data required for contracted services.*
4. **For the Regular Exercise of Rights in Legal, Administrative, or Arbitral Proceedings:** Data necessary for legal defenses and rights enforcement. *Example: Information for legal proceedings.*
5. **To Protect the Life or Physical Safety of the Data Subject or a Third Party:** Data processed in emergencies to ensure life or physical integrity. *Example: Data sharing in medical emergencies.*
6. **For Health Protection, Exclusively Performed by Health Professionals or Authorities:** Data processed in health-related procedures. *Example: Medical data shared with health professionals.*

7. **To Serve Legitimate Interests:** Data processed for legitimate interests of the controller or third parties, provided rights and freedoms of the data subject are not overridden. *Example: Service improvement analysis, fraud prevention.*

3. Purposes of Data Processing: [Organization Name] processes personal data for the following purposes:

1. **To Provide Services:** Collection and use of data to deliver contracted services. *Example: Name, email address, phone number, payment information.*
2. **To Comply with Legal and Regulatory Obligations:** Ensuring compliance with legal and regulatory requirements. *Example: Storage of tax and accounting records.*
3. **For Communications and Marketing:** Sending promotional and marketing communications with consent. *Example: Marketing emails, newsletters.*
4. **To Improve Services:** Analyzing data to enhance and develop new services. *Example: Customer feedback, service usage analysis.*

4. Form and Duration of Data Processing:

- **Form:** Personal data is processed securely and confidentially using technologies and processes that ensure protection against unauthorized access, loss, alteration, or misuse.
- **Duration:** Personal data is stored as long as necessary to fulfill the purposes for which it was collected, considering contract terms, legal and regulatory deadlines, or while consent remains valid. After the processing period, data will be deleted, anonymized, or securely stored in compliance with the law.

5. Data Sharing: Personal data may be shared in the following situations:

- With Service Providers: Acting on our behalf for specific activities.
- With Government Authorities: When required by law or to protect rights.
- With Partner Companies: For marketing purposes, with the consent of the data subject.

6. Data Security: Technical and administrative measures are adopted to protect personal data against unauthorized access, loss, alteration, or misuse.

7. Data Subject Rights: The data subject has the following rights:

- Confirm data processing existence.
- Access their personal data.
- Request correction, anonymization, or deletion of unnecessary data.
- Data portability to another service provider.
- Withdraw consent at any time.

8. Consent Terms: By accepting this Privacy Policy, the data subject consents to data processing for the purposes outlined above. Consent can be revoked upon request.

9. Policy Changes: [Organization Name] reserves the right to modify this policy. Changes will be published on our website.

10. Contact Information: For inquiries or to exercise rights, contact us at [email address], [phone number], or [physical address].

Effective Date: This Privacy Policy is effective from its publication date on our website.

—

T-02: Is the processing of personal data carried out according to a legal basis?

Legal Basis for the Processing of Personal Data

[Organization Name] processes personal data based on the following legal grounds, in accordance with Article 7 of the LGPD:

1. **With the Consent of the Data Subject**

   Description: Personal data processing is carried out with the free, informed, and unequivocal consent of the data subject. This consent must be provided clearly and prominently so that the data subject is fully aware of the specific purposes for which their data is being collected and processed.

   Example: Sending newsletters, promotional communications, participation in satisfaction surveys.

2. **For Compliance with a Legal or Regulatory Obligation by the Controller**

   Description: We use personal data to fulfill legal and regulatory obligations imposed by current legislation. This includes collecting and storing information necessary to meet the requirements of governmental and regulatory bodies.

   Example: Storage of tax and accounting data, information for audit purposes, provision of data to tax or regulatory authorities.

3. **For the Execution of a Contract or Preliminary Procedures Related to a Contract**

   Description: We process personal data necessary for the execution of contracts in which the data subject is a party or for preliminary procedures related to contracts. These data are essential to ensure the correct provision of contracted services and the execution of contractual obligations.

   Example: Data necessary for the provision of contracted services, preparation of commercial proposals, communication with clients during the contract term.

4. **For the Regular Exercise of Rights in Judicial, Administrative, or Arbitration Procedures**

   Description: We process personal data necessary to protect our rights in judicial, administrative, or arbitration proceedings. This includes collecting and using data for defense or exercise of rights in legal or regulatory disputes.

   Example: Information for legal defense, presentation of evidence in litigation, compliance with court orders.

5. **To Protect the Life or Physical Safety of the Data Subject or Third Party**

   Description: We process personal data in emergency situations to protect the life or physical integrity of the data subject or third parties. These situations require a quick and effective response to prevent harm or risks to health and safety.

   Example: Sharing data in medical emergencies, communicating relevant information to emergency services or competent authorities.

6. **For the Protection of Health, Exclusively in Procedures Performed by Health Professionals, Health Services, or Health Authority**

   Description: We process personal data for health protection in procedures carried out by health professionals or health authorities. These data are essential to ensure the quality and safety of healthcare provided to data subjects.

   Example: Medical data shared with health professionals, recording medical history for ongoing treatment, communication with health authorities in case of public health emergencies.

7. **When Necessary to Meet the Legitimate Interests of the Controller or Third Party**

   Description: We use personal data to meet the legitimate interests of the controller or third parties, except when overridden by the fundamental rights and freedoms of the data subject that require personal data protection. This legal basis allows data processing for legitimate purposes that do not harm the rights and interests of data subjects.

   Example: Service improvement analysis, fraud prevention, security monitoring, targeted marketing activities, development of new products and services.

—

T-03: Does the system inform the data subject about the purposes of personal data processing?

Purposes of Data Processing

[Organization Name] processes personal data for the following purposes:

1. **To Provide Services:**

   Description: We collect and use personal data to provide our services as contracted by the data subjects. This processing is essential for the execution of the contract or preliminary procedures related to it, as requested by the data subject.

   Example: Name, email address, phone number, payment information.

2. **To Comply with Legal and Regulatory Obligations:**

   Description: We use personal data to comply with legal and regulatory obligations, ensuring conformity with the requirements of competent authorities. This processing is necessary for fulfilling a legal obligation to which the controller is subject.

   Example: Storage of tax and accounting data.

3. **For Communications and Marketing:**

   Description: We may use personal data to send promotional and marketing communications, provided we have obtained prior consent from the data subject. This processing aims to inform the data subject about products, services, special offers, and events that may be of interest.

   Example: Marketing emails, newsletters.

4. **To Improve Services:**

   Description: We analyze personal data to improve our services and develop new products and services. This processing is based on the legitimate interest of [Organization Name] in ensuring the continuous quality and innovation of our services.

   Example: Customer feedback, service usage analysis.

5. **To Personalize the User Experience:**

   Description: We use personal data to personalize the user experience, offering content, recommendations, and services tailored to their preferences and needs. This processing is based on the legitimate interest of providing a more relevant and satisfying experience to the data subject.

   Example: Browsing preferences, purchase history, content personalization.

6. **For Customer Relationship Management (CRM):**

   Description: We process personal data to manage our relationship with customers, providing support, resolving issues, and improving customer satisfaction. This processing is necessary for the execution of the contract and for improving the quality of the service provided.

   Example: Contact data, interaction history, service preferences.

7. **For Recruitment and Personnel Selection:**

   Description: We use personal data for recruitment and selection processes, including candidate evaluation and communication during the selection process. This processing is necessary for the execution of pre-contractual procedures requested by the data subject.

   Example: Resumes, professional history, candidate assessments.

8. **To Ensure System Security and Integrity:**

   Description: We process personal data to ensure the security and integrity of our systems, preventing fraud, unauthorized access, and other threats. This processing is based on the legitimate interest of protecting our technological resources and sensitive data.

   Example: Access logs, authentication information, security monitoring.

—

T-04: Does the system process data in compliance with the purposes presented to the data subject?

Step-by-Step Guide to Review Consent and Implement Changes

1. **Identify the Declared Purposes:** Clearly list each purpose and associate it with the specific data collected for each purpose.
2. **Audit the Collected Data:** Compare the data collected with the declared purposes to identify any unnecessary or undisclosed data collection.
3. **Review Obtained Consents:** Analyze the consent documents obtained from the data subjects to ensure they were adequately informed about the purposes of data processing. Ensure that consents are specific, informed, and freely provided.
4. **Evaluate Compliance with LGPD:** Identify any data processing activities that are not aligned with the declared purposes or are not compliant with the LGPD.
5. **Implement Corrections:** Stop collecting unnecessary or unauthorized data and, if necessary, delete any data that was improperly collected. Update privacy policies and terms of use to accurately reflect the purposes of processing. If required, request new consent from the data subjects for the corrected and updated purposes.

6. **Communicate with the Data Subjects:** Send clear and understandable notifications to the data subjects about the implemented changes. Offer data subjects the option to withdraw their consent if they do not agree with the new purposes.
7. **Documentation and Record-Keeping:** Maintain detailed records of all data processing activities, including the changes made. Store all updated consent documents.
8. **Continuous Monitoring:** Conduct periodic audits to ensure ongoing compliance with the declared purposes and the LGPD. Regularly review and update privacy policies and terms of use as necessary.

—

T-05: Does the system inform the data subject about the form and duration of their personal data processing in a free and accessible manner?

Form and Duration of Data Processing

1. **Form of Data Processing:** Personal data is processed securely and confidentially, using technologies and procedures that ensure protection against unauthorized access, loss, destruction, alteration, or any form of improper or unlawful processing. Processing operations include, but are not limited to, collection, storage, use, sharing, updating, and deletion of data.
2. **Duration of Data Processing:** Personal data will be processed and stored for as long as necessary to fulfill the purposes for which it was collected, observing the following:
   - The duration of contracts with the data subjects.
   - Applicable legal and regulatory deadlines.
   - The period required for the defense of rights in judicial, administrative, or arbitration proceedings.
   - While the consent of the data subject remains valid, when applicable.

   After the processing period ends, personal data will be deleted, anonymized, or securely stored in compliance with applicable legislation.

—

T-06: Does the system allow the data subject to consult the entirety of their personal data in a free and accessible manner?

Personal Data Access Request Form

Data Subject Information:

- **Full Name:** ________________________
- **CPF:** ________________________
- **Email:** ________________________
- **Phone:** ________________________
- **Address:** ________________________

Request: I, [Data Subject's Name], hereby exercise my right to access my personal data, as provided by the General Data Protection Law (LGPD) - Law No. 13,709/2018. I request the following information:

1. **Confirmation of Processing:** Confirm whether my personal data is being processed by this organization.
2. **Access to Data:** Provide a copy of all personal data this organization holds about me, including but not limited to:
    - Registration data
    - Transaction history
    - Interaction and communication data
    - Any other personal data maintained by the organization
3. **Information about Processing:** Clarifications regarding the following:
    - Purposes of processing my personal data
    - Storage period of personal data or, if not possible, the criteria used to define this period
    - Information about the origin of the data, if not collected directly from me
4. **Response Methods:** I request that the response to this request be sent to the email address __________________________.
5. **Declaration and Signature:** I declare that the information provided in this form is true and accurate. I understand that it may be necessary to prove my identity for this request to be processed.

—

T-07: Does the system store personal data collected from data subjects with accuracy and clarity?

To ensure that personal data of data subjects is stored accurately and clearly, it is essential to implement best programming practices both on the front-end and back-end. Below are some suggestions that can be applied to achieve this goal.

Front-End Best Practices

1. **Form Validation:** Use form validation libraries such as Formik and Yup (React) or Vuelidate (Vue.js) to ensure that user-entered data is in the correct format before being sent to the server.

```
import * as Yup from 'yup';

const validationSchema = Yup.object().shape({
  nome: Yup.string().required('Name is required'),
  email: Yup.string().email('Invalid email').required('Email is required'),
  cpf: Yup.string().matches(/^\d{3}\.\d{3}\.\d{3}\-\d{2}$/, 'Invalid CPF')
    .required('CPF is required'),
});
```

2. **Input Masks:** Use input masks for sensitive fields such as CPF, phone numbers, and dates to ensure data is entered in the correct format.

```
import InputMask from ’react-input-mask’;

<InputMask mask="999.999.999-99" value={this.state.cpf}
    onChange={this.handleChange}>
  {(inputProps) => <input {...inputProps} type="text" />}
</InputMask>
```

3. **User Feedback:** Provide real-time feedback to users about the validity of the data entered, using clear and specific error messages.

```
<div className="error">
    {errors.nome && touched.nome && <span>{errors.nome}</span>}
</div>
```

4. **Front-End Security:** Ensure that sensitive data is not stored in localStorage or sessionStorage, as these locations can be easily accessed by malicious scripts.

Back-End Best Practices

1. **Validation and Sanitization:** On the back-end, validate and sanitize all data received from the front-end to prevent SQL injection, XSS, and other vulnerabilities. Use libraries such as Joi (Node.js) or Validator (Python).

```
const Joi = require(’joi’);

const schema = Joi.object({
  nome: Joi.string().min(3).max(30).required(),
  email: Joi.string().email().required(),
  cpf: Joi.string().pattern(/^\d{3}\.\d{3}\.\d{3}\-\d{2}$/).required(),
});

const { error, value } = schema.validate(req.body);
if (error) {
  return res.status(400).send(error.details[0].message);
}
```

2. **Secure Storage:** Use encryption to store sensitive data in the database. For passwords, use hashing algorithms such as bcrypt.

```
const bcrypt = require(’bcrypt’);

const saltRounds = 10;
const hashedPassword = await bcrypt.hash(password, saltRounds);
```

3. **Audit Logs:** Implement audit logs to monitor who accessed or modified personal data. Ensure that logs are protected against unauthorized changes.

4. **Access Control:** Implement role-based access control (RBAC) to ensure that only authorized users can access or modify personal data.

5. **Performance and Integrity:** Use database transactions to ensure data integrity in critical operations.

```
const { Pool } = require('pg');
const pool = new Pool();

async function executeTransaction() {
  const client = await pool.connect();
  try {
    await client.query('BEGIN');
    const queryText = 'INSERT INTO users(name, email)
        VALUES($1, $2) RETURNING id';
    const res = await client.query(queryText,
        ['John Doe', 'johndoe@example.com']);
    await client.query('COMMIT');
    return res.rows[0];
  } catch (e) {
    await client.query('ROLLBACK');
    throw e;
  } finally {
    client.release();
  }
}
```

—

T-08: Does the system keep personal data updated as necessary to fulfill the purpose of its processing?

Process for Mapping and Reviewing Personal Data

1. **Identification and Cataloging of Personal Data:**
   - Conduct a comprehensive survey of all sources of personal data.
   - Catalog the types of personal data.
   - Record the purposes for which each type of personal data is collected and used.
   - Identify the individuals responsible for processing each set of data.
2. **Defining Review Frequency:**
   - Set the review frequency according to the criticality and nature of the data.
   - Take into account current legislation and best practices.
3. **Implementation of Update Mechanisms:**
   - Develop and implement data update forms for data subjects.
   - Create automatic reminders to encourage data subjects to update their data regularly.
   - Facilitate access for data subjects to review and correct their data.

4. **Auditing and Verification:**
    - Conduct periodic audits to verify data compliance with the declared purposes.
    - Use sampling techniques to review data in large-scale systems.
5. **Change Logs and Reporting:**
    - Record all changes made to personal data.
    - Maintain detailed logs of access and modifications.

—

T-09: Does the system provide the data subject with information about data processing and the identity of the controller?

Data Protection Officer (DPO) Communication Center

The organization provides the following channels to ensure data subjects can access information about the processing of their personal data and the identity of the controller:

- **Contact by Email:** For inquiries or requests related to privacy and data protection, send an email to: `dpo@company.com`
- **Contact by Phone:** Data subjects can contact the organization directly via phone at: `+55 01 2345-6789` *Availability: Monday to Friday, 9:00 AM to 6:00 PM.*
- **Online Chat:** For immediate support, an online chat service is available. Users can initiate a conversation with a representative by clicking the designated button on the organization's website. Example of chat service integration:

HTML Example for Online Communication

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Data Protection Officer Communication Center</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            background-color: #f4f4f4;
        }
        .container {
            max-width: 800px;
            margin: auto;
            background-color: #fff;
            padding: 20px;
            box-shadow: 0 0 10px rgba(0, 0, 0, 0.1);
        }
    </style>
</head>
<body>
    <div class="container">
        <h1>Data Protection Officer Communication Center</h1>
        <p>Contact us via email, phone, or chat for data-related inquiries.</p>
    </div>
</body>
</html>
```

Additional Notes: The organization ensures that all communication methods are secure and accessible, providing timely responses to inquiries about the identity of the data controller, processing activities, and the rights of the data subject.

—

T-10: Does the organization process data, when based on legitimate interest, in compliance with the law?

To determine whether data processing can be based on the legal ground of legitimate interest under the LGPD, follow these steps:

1. **Define Legitimate Interest:**
    - Clearly identify and describe the legitimate interest of the organization.
    - Justify the necessity and validity of the interest, ensuring it is specific, ethical, and aligned with the expectations of the data subjects.
2. **Analyze the Necessity of Processing:**
    - Evaluate whether data processing is strictly necessary to achieve the legitimate interest.
    - Verify if there are alternatives that do not involve personal data processing and ensure the collection is proportionate to the objective.
3. **Assess the Impact on Data Subjects' Rights:**
    - Analyze potential risks and negative impacts on the rights and freedoms of the data subjects.
    - Weigh the organization's legitimate interest against the rights of the data subjects, ensuring the interest justifies the risks and that adequate safeguards are in place.
4. **Ensure Transparency and Documentation:**
    - Inform data subjects about processing based on legitimate interest, including detailed information in privacy notices.
    - Document the entire analysis process, maintaining detailed records for audits or inquiries.
5. **Perform Periodic Reviews and Monitoring:**
    - Periodically review data processing activities and the legitimate interest analysis, updating documentation as necessary.

- Implement continuous monitoring mechanisms to ensure ongoing compliance with the LGPD.

Conclusion: By following these steps, the organization can clearly and thoroughly demonstrate that data processing based on legitimate interest is justified, necessary, and non-prejudicial to the rights of data subjects, ensuring compliance with the LGPD.

—

T-11: Does the system keep records of data processing operations, especially when based on legitimate interest?

To maintain records of data processing operations in compliance with the General Data Protection Law (LGPD), a database table can be created to log these operations. Below is an example SQL script for creating a table named `operacoes_tratamento_dados` along with its respective columns.

SQL Script: Creating the Database and Table

```
-- Create the database
CREATE DATABASE IF NOT EXISTS lgpd_registros;

-- Select the database
USE lgpd_registros;

-- Create the table to record data processing operations
CREATE TABLE IF NOT EXISTS operacoes_tratamento_dados (
    id_operacao INT AUTO_INCREMENT PRIMARY KEY,
    tipo_operacao VARCHAR(255) NOT NULL,
    descricao_operacao TEXT NOT NULL,
    data_hora_operacao TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    usuario_responsavel VARCHAR(255) NOT NULL,
    ip_usuario VARCHAR(45),
    dados_envolvidos TEXT,
    resultado_operacao VARCHAR(255)
);

-- Create an index to facilitate queries by date and operation type
CREATE INDEX idx_data_tipo_operacao ON operacoes_tratamento_dados
    (data_hora_operacao, tipo_operacao);
```

Column Descriptions:

- **id_operacao:** Unique identifier for each data processing operation.
- **tipo_operacao:** Type of operation performed (e.g., creation, update, deletion, access).
- **descricao_operacao:** Detailed description of the operation performed.
- **data_hora_operacao:** Date and time when the operation was performed. Default value is the current timestamp.
- **usuario_responsavel:** Identification of the user responsible for the operation.

- **ip_usuario:** IP address of the user who performed the operation (optional).
- **dados_envolvidos:** Specific data involved in the operation (optional).
- **resultado_operacao:** Outcome of the operation performed (e.g., success, failure).

Examples of Data Insertion:

```
-- Insert a creation operation
INSERT INTO operacoes_tratamento_dados
(tipo_operacao, descricao_operacao, usuario_responsavel, ip_usuario,
    dados_envolvidos, resultado_operacao)
VALUES
('creation', 'Creation of a new user record', 'admin', '192.168.0.1',
    'Name: João, Email: joao@example.com', 'success');

-- Insert an update operation
INSERT INTO operacoes_tratamento_dados
(tipo_operacao, descricao_operacao, usuario_responsavel, ip_usuario,
    dados_envolvidos, resultado_operacao)
VALUES
('update', 'Update of a user email address', 'admin', '192.168.0.1',
    'Old Email: joao@example.com, New Email: joao2@example.com', 'success');

-- Insert a deletion operation
INSERT INTO operacoes_tratamento_dados
(tipo_operacao, descricao_operacao, usuario_responsavel, ip_usuario,
    dados_envolvidos, resultado_operacao)
VALUES
('deletion', 'Deletion of a user record', 'admin', '192.168.0.1',
    'Name: João, Email: joao2@example.com', 'success');
```

Conclusion: This script provides a foundation for logging data processing operations in a MySQL database, facilitating LGPD compliance. Depending on the specific needs of your system, additional columns can be added, or the structure can be adjusted accordingly.

—

T-12: Does the system inform the data subject and the relevant authorities about data processing, especially when based on legitimate interest?

Data Processing Operations Report

1. **Organization Identification:**
   - Organization Name:
   - CNPJ:
   - Address:

- Data Protection Officer (DPO):
- Contact Email:
- Contact Phone:

2. **General Description of Data Processing Activities:**
    - Purpose of Data Processing:
    - Legal Basis for Processing:
    - Categories of Personal Data Processed:
    - Categories of Data Subjects:
3. **Data Collection Procedures:**
    - Methods of Data Collection: (e.g., online forms, in-person collection, etc.)
    - Data Retention Period:
    - Anonymization Process (if applicable):
4. **Data Sharing:**
    - Third Parties with Whom Data is Shared:
    - Purpose of Data Sharing:
    - Security Measures for Sharing:
5. **Security and Data Protection Measures:**
    - Description of Technical and Administrative Measures: (e.g., encryption, access control, etc.)
    - Backup and Data Recovery Policy:
    - Incident Response Plans:
    - Employee Training and Awareness Programs:
6. **Data Subject Rights:**
    - Procedures for Data Subject Requests:
    - Number of Requests Received and Addressed:
    - Most Common Types of Requests:
7. **Security Incident Reports:**
    - Incident Description:
    - Incident Impact:
    - Mitigation and Correction Measures Adopted:
    - Communication with Data Subjects and Authorities:
8. **Data Protection Impact Assessment (DPIA):**
    - Description of Assessments Conducted:
    - Identified Risks and Mitigation Measures:
    - Date of Last Assessment:

9. **Audits and Compliance:**
    - Date of Last Internal Audits:
    - Conclusions and Recommendations:
    - Action Plans for Improvements:
10. **Final Statement:**
    - Declaration of Compliance with LGPD:
    - Name and Signature of Responsible Party:
    - Report Date:

—

T-13: Does the system process personal or sensitive data in a way that it cannot be linked to a data subject when requested?

To address the demand for processing personal or sensitive data in a manner that cannot be linked to a data subject, it is essential to implement anonymization and pseudonymization techniques. Below are some insights that may be useful in this context:

Anonymization Techniques

- **Generalization:**
    - **Description:** Modify attribute values to make them less specific.
    - **Example:** Change a birth date from "15/06/1990" to "1990" or "the 1990s."
- **Suppression:**
    - **Description:** Completely remove some attributes or parts of attributes.
    - **Example:** Remove identification numbers, such as CPF, or parts of an address.
- **Perturbation:**
    - **Description:** Introduce noise or slightly alter data to prevent identification.
    - **Example:** Add or subtract a small random value to ages.
- **Data Shuffling:**
    - **Description:** Shuffle attribute values among different records.
    - **Example:** Swap postal addresses between different individuals in the dataset.
- **Masking:**
    - **Description:** Replace real data with fictitious values.
    - **Example:** Replace real names with generic names like "User A," "User B."

Pseudonymization Techniques

- **Substitution of Direct Identifiers:**

  - **Description:** Replace unique identifiers with pseudonyms.
  - **Example:** Replace a CPF number with a randomly generated code.
- **Encryption:**
  - **Description:** Use encryption techniques to protect sensitive data.
  - **Example:** Encrypt health data with keys that only authorized entities can decrypt.
- **Tokenization:**
  - **Description:** Replace sensitive data with tokens that can only be reversed with the correct key.
  - **Example:** Replace a credit card number with a specific token.

Additional Best Practices

- **Data Minimization:**
  - **Description:** Collect and retain only the data necessary for the specific purpose.
  - **Example:** Collect only age instead of the full birth date when only the age group is needed.
- **Regular Auditing:**
  - **Description:** Conduct periodic audits to ensure that anonymization and pseudonymization processes are effective and that there is no possibility of re-identification.
  - **Example:** Test anonymized datasets to verify their resistance to re-identification.
- **Documentation:**
  - **Description:** Maintain detailed documentation of the anonymization and pseudonymization methods used, as well as data protection policies.
  - **Example:** Record the techniques applied to each dataset and the justifications for their selection.
- **Awareness:**
  - **Description:** Train employees on the importance of data protection and how to correctly implement anonymization and pseudonymization techniques.
  - **Example:** Continuous training programs on LGPD and data security practices.

—

T-14: Does the system inform the data subject about the existence of data processing prior to collection?

Notice of Collection and Processing of Personal Data

Dear [Data Subject's Name],

In compliance with the General Data Protection Law (Law No. 13,709/2018 - LGPD), we inform you that [Company/Organization Name] will collect and process your personal data for the purpose of [specify the purpose of processing].

1. Purpose of Data Collection and Processing The data collected will be used for the following purposes:

- Describe the specific purpose
- Describe another purpose, if applicable

2. Data Collected The following personal data may be collected:

- List the types of data, e.g., name, email, phone number, etc.

3. Data Sharing Your data may be shared with the following partners/third parties, as necessary:

- Name of partner/third party and purpose of sharing

4. Data Subject Rights As a data subject, you have the following rights:

- Access to your data.
- Correction of incomplete, inaccurate, or outdated data.
- Anonymization, blocking, or deletion of unnecessary, excessive, or unlawfully processed data.
- Portability of your data to another service or product provider.
- Deletion of data processed with your consent.
- Information about the sharing of your data with public and private entities.
- Information about the possibility of not providing consent and the consequences of refusal.
- Revocation of consent, as provided by the LGPD.

5. Data Security We adopt appropriate technical and administrative measures to protect the personal data collected against unauthorized access, accidental or unlawful situations of destruction, loss, alteration, communication, or any form of improper or unlawful processing.

6. Contact for More Information If you have any questions about the processing of your personal data, please contact us at [contact email] or phone [phone number].

Consent Request To proceed with the collection and processing of your personal data, we request your consent. If you agree, please check the box below and click continue.

( ) I agree with the collection and processing of my personal data as described above.

—

E.2 Consent Templates

C-01: Does the system allow the data subject to provide consent autonomously and clearly for the processing of their data?

In the Consent Form, it is recommended to use clear, objective, and accessible language, avoiding any technical or complex jargon that could hinder the data subject's understanding. It is essential that all information is presented transparently and directly, ensuring that the data subject fully understands how their data will be used and for what purposes.

Moreover, it is crucial to avoid any form of misleading or ambiguous messaging that might lead the data subject to errors or misinterpretations. Consent must be obtained ethically and responsibly, ensuring that the data subject has a complete and truthful view of the personal data processing process.

Another important practice is to refrain from using pre-checked boxes to obtain consent. The data subject's choice must be explicitly expressed through a clear affirmative action, such as marking an empty checkbox, so there is no doubt about their intent to consent. This reinforces the autonomy and control of the data subject over their personal data.

Finally, it is imperative to include a clear and easily accessible option for the data subject to deny or withdraw their consent at any time, without suffering any prejudice or discrimination as a result of this decision. This option should be explicitly communicated in the consent form, along with instructions on how to withdraw consent. Respect for the data subject's wishes is fundamental to complying with the principles of the General Data Protection Law (LGPD) and building a relationship of trust between the organization and the individuals whose data is processed.

—

C-02: Does the system request the data subject's specific consent to communicate or share personal data with other controllers?

It is mandatory to be transparent with the data subject regarding the purpose of processing their data. Transparency involves providing detailed and comprehensible information about why and how personal data will be used, ensuring that the data subject is fully aware of the processing activities from the outset.

Especially when sharing data with other controllers, the data subject must be clearly and specifically informed in the consent form. This includes identifying which data will be shared, the identity of the third parties with whom the data will be shared, and the specific purposes for which these third parties will use the data.

The communication must be direct and unambiguous, ensuring that the data subject fully understands all implications of sharing their data. Consent for sharing must be explicit and separate from other processing purposes, allowing the data subject granular control over their choices. Additionally, the data subject must be informed of any potential risks associated with the sharing of their data, as well as the security measures adopted to protect their information.

This approach not only meets the legal requirements of the General Data Protection Law (LGPD) but also promotes trust and transparency between the organization and the data subjects. Transparency in data processing and sharing is fundamental to protecting the rights of data subjects and building a relationship of trust and mutual respect.

—

C-03: Does the system store the consent provided by the data subject for legal evidence?

Database Structure

To implement consent storage, a simple database structure using PostgreSQL can be employed. Below is an example that includes a main table, `consents`, to store consents provided by data subjects.

```
CREATE TABLE users (
    id SERIAL PRIMARY KEY,
    name VARCHAR(100) NOT NULL,
    email VARCHAR(100) UNIQUE NOT NULL,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

CREATE TABLE consents (
    id SERIAL PRIMARY KEY,
    user_id INTEGER REFERENCES users(id) ON DELETE CASCADE,
    consent_given BOOLEAN NOT NULL,
    consent_text TEXT NOT NULL,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    revoked_at TIMESTAMP
);
```

Backend with Node.js and Express

The backend uses Node.js with the Express framework to create an API for storing and managing consents.

Directory Structure:

```
/backend
  |-- index.js
  |-- db.js
  |-- routes
      |-- users.js
      |-- consents.js
```

index.js:

```
const express = require('express');
const app = express();
const usersRouter = require('./routes/users');
const consentsRouter = require('./routes/consents');

app.use(express.json());
app.use('/users', usersRouter);
app.use('/consents', consentsRouter);

const PORT = process.env.PORT || 3000;
app.listen(PORT, () => {
    console.log(‘Server is running on port ${PORT}‘);
});
```

db.js:

```
const { Pool } = require('pg');

const pool = new Pool({
    user: 'yourusername',
    host: 'localhost',
    database: 'yourdatabase',
    password: 'yourpassword',
    port: 5432,
});

module.exports = pool;
```

routes/users.js:

```
const express = require('express');
const router = express.Router();
const pool = require('../db');

router.post('/', async (req, res) => {
    const { name, email } = req.body;
    try {
        const newUser = await pool.query(
            'INSERT INTO users (name, email) VALUES ($1, $2) RETURNING *',
            [name, email]
        );
        res.json(newUser.rows[0]);
    } catch (err) {
        res.status(500).send(err.message);
    }
});

module.exports = router;
```

routes/consents.js:

```
const express = require('express');
const router = express.Router();
const pool = require('../db');

router.post('/', async (req, res) => {
    const { user_id, consent_given, consent_text } = req.body;
    try {
        const newConsent = await pool.query(
            'INSERT INTO consents (user_id, consent_given, consent_text)
            VALUES ($1, $2, $3) RETURNING *',
            [user_id, consent_given, consent_text]
        );
        res.json(newConsent.rows[0]);
    } catch (err) {
        res.status(500).send(err.message);
    }
});

router.put('/revoke/:id', async (req, res) => {
    const { id } = req.params;
    try {
        const revokedConsent = await pool.query(
            'UPDATE consents SET revoked_at = CURRENT_TIMESTAMP
            WHERE id = $1 RETURNING *',
            [id]
        );
        res.json(revokedConsent.rows[0]);
    } catch (err) {
        res.status(500).send(err.message);
    }
});

module.exports = router;
```

Frontend with React

For the frontend, React is used to create a simple interface for collecting and managing consents.

Directory Structure:

```
/frontend
  |-- src
      |-- App.js
      |-- components
          |-- ConsentForm.js
```

App.js:

```
import React from 'react';
import ConsentForm from './components/ConsentForm';

function App() {
  return (
    <div className="App">
      <h1>Consent Management</h1>
      <ConsentForm />
    </div>
  );
}
```

```
export default App;
```

components/ConsentForm.js:

```
import React, { useState } from 'react';
import axios from 'axios';

function ConsentForm() {
  const [name, setName] = useState('');
  const [email, setEmail] = useState('');
  const [consent, setConsent] = useState(false);
  const [consentText, setConsentText] =
    useState('I agree to the terms of use for my personal data.');

  const handleSubmit = async (e) => {
    e.preventDefault();
    try {
      const userResponse = await axios.post('/users', { name, email });
      const userId = userResponse.data.id;
      await axios.post('/consents', { user_id: userId,
        consent_given: consent, consent_text: consentText });
      alert('Consent successfully recorded.');
    } catch (err) {
      console.error(err);
      alert('Error recording consent.');
    }
  };

  return (
    <form onSubmit={handleSubmit}>
      <div>
        <label>Name:</label>
        <input type="text" value={name} onChange={(e) =>
            setName(e.target.value)} required />
      </div>
      <div>
        <label>Email:</label>
        <input type="email" value={email} onChange={(e) =>
            setEmail(e.target.value)} required />
      </div>
      <div>
        <label>Consent:</label>
        <input type="checkbox" checked={consent} onChange={(e) =>
            setConsent(e.target.checked)} />
        {consentText}
      </div>
      <button type="submit">Submit</button>
    </form>
  );
}

export default ConsentForm;
```

—

C-04: Does the system provide data subjects with means to refuse or withdraw consent without prejudice?

Frontend with React: Adding an Interface for Consent Withdrawal

To allow data subjects to refuse or withdraw consent without prejudice, an interface can be added to the frontend alongside the example provided in item **C-03**.

Updated Directory Structure:

```
/src
  |-- App.js
  |-- components
      |-- ConsentForm.js
      |-- RevokeConsent.js
```

App.js:

```
import React from 'react';
import ConsentForm from './components/ConsentForm';
import RevokeConsent from './components/RevokeConsent';

function App() {
  return (
    <div className="App">
      <h1>Consent Management</h1>
      <ConsentForm />
      <RevokeConsent />
    </div>
  );
}

export default App;
```

components/ConsentForm.js:

```
import React, { useState } from 'react';
import axios from 'axios';

function ConsentForm() {
  const [name, setName] = useState('');
  const [email, setEmail] = useState('');
  const [consent, setConsent] = useState(false);
  const [consentText, setConsentText] =
    useState('I agree to the terms of use for my personal data.');

  const handleSubmit = async (e) => {
    e.preventDefault();
    try {
      const userResponse = await axios.post('/users', { name, email });
      const userId = userResponse.data.id;
      await axios.post('/consents', { user_id: userId,
        consent_given: consent, consent_text: consentText });
      alert('Consent successfully recorded.');
    } catch (err) {
      console.error(err);
      alert('Error recording consent.');
    }
  };

  return (
    <form onSubmit={handleSubmit}>
      <div>
        <label>Name:</label>
        <input type="text" value={name} onChange={(e) =>
            setName(e.target.value)} required />
      </div>
      <div>
        <label>Email:</label>
        <input type="email" value={email} onChange={(e) =>
            setEmail(e.target.value)} required />
      </div>
      <div>
        <label>Consent:</label>
        <input type="checkbox" checked={consent} onChange={(e) =>
            setConsent(e.target.checked)} />
        {consentText}
      </div>
      <button type="submit">Submit</button>
    </form>
  );
}

export default ConsentForm;
```

components/RevokeConsent.js:

```
import React, { useState } from 'react';
import axios from ’axios’;

function RevokeConsent() {
  const [email, setEmail] = useState(’’);

  const handleRevoke = async (e) => {
    e.preventDefault();
    try {
      const response = await axios.get(‘/users?email=${email}‘);
      const userId = response.data.id;
      await axios.put(‘/consents/revoke/${userId}‘);
      alert(’Consent successfully revoked.’);
    } catch (err) {
      console.error(err);
      alert(’Error revoking consent.’);
    }
  };

  return (
    <form onSubmit={handleRevoke}>
      <h2>Revoke Consent</h2>
      <div>
        <label>Email:</label>
        <input type="email" value={email} onChange={(e) =>
            setEmail(e.target.value)} required />
      </div>
      <button type="submit">Revoke Consent</button>
    </form>
  );
}

export default RevokeConsent;
```

Backend Updated with Node.js and Express

routes/users.js:

```
const express = require(’express’);
const router = express.Router();
const pool = require(’../db’);

router.post(’/’, async (req, res) => {
    const { name, email } = req.body;
    try {
        const newUser = await pool.query(
            ’INSERT INTO users (name, email) VALUES ($1, $2) RETURNING *’,
            [name, email]
        );
        res.json(newUser.rows[0]);
    } catch (err) {
        res.status(500).send(err.message);
    }
});

router.get('/', async (req, res) => {
    const { email } = req.query;
    try {
        const user = await pool.query(
            'SELECT * FROM users WHERE email = $1',
            [email]
        );
        if (user.rows.length > 0) {
            res.json(user.rows[0]);
        } else {
            res.status(404).send('User not found.');
        }
    } catch (err) {
        res.status(500).send(err.message);
    }
});

module.exports = router;
```

routes/consents.js:

```
const express = require('express');
const router = express.Router();
const pool = require('../db');

router.post('/', async (req, res) => {
    const { user_id, consent_given, consent_text } = req.body;
    try {
        const newConsent = await pool.query(
            'INSERT INTO consents (user_id, consent_given, consent_text)
                VALUES ($1, $2, $3) RETURNING *',
            [user_id, consent_given, consent_text]
        );
        res.json(newConsent.rows[0]);
    } catch (err) {
        res.status(500).send(err.message);
    }
});

router.put('/revoke/:user_id', async (req, res) => {
    const { user_id } = req.params;
    try {
        const revokedConsent = await pool.query(
            'UPDATE consents SET revoked_at = CURRENT_TIMESTAMP
                WHERE user_id = $1 AND revoked_at IS NULL RETURNING *',
            [user_id]
        );
        if (revokedConsent.rows.length > 0) {
            res.json(revokedConsent.rows[0]);
        } else {
            res.status(404).send('Consent not found or already revoked.');
        }
    } catch (err) {
        res.status(500).send(err.message);
    }
});

module.exports = router;
```

Conclusion: This updated example includes a frontend interface for the data subject to revoke consent and backend endpoints for retrieving users by email and revoking consent. This ensures the data subject can easily withdraw consent without prejudice.

—

C-05: Does the system process the personal data of children and adolescents only with specific consent from parents or legal guardians, in an accessible and easy-to-understand manner?

Update to the Consent Interface

The consent form example from item **C-03** can be updated to include a checkbox confirming that the user is of legal age. This ensures that consent is given legally and appropriately when dealing with the personal data of children and adolescents.

Updated Code for `components/ConsentForm.js`:

```
import React, { useState } from 'react';
import axios from 'axios';

function ConsentForm() {
  const [name, setName] = useState('');
  const [email, setEmail] = useState('');
  const [consent, setConsent] = useState(false);
  const [isAdult, setIsAdult] = useState(false);
  const [consentText, setConsentText] =
    useState('I agree to the terms of use for my personal data.');

  const handleSubmit = async (e) => {
    e.preventDefault();
    if (!isAdult) {
      alert('You must confirm that you are of legal age.');
      return;
    }
    try {
      const userResponse = await axios.post('/users', { name, email });
      const userId = userResponse.data.id;
      await axios.post('/consents', { user_id: userId,
        consent_given: consent, consent_text: consentText });
      alert('Consent successfully recorded.');
    } catch (err) {
      console.error(err);
      alert('Error recording consent.');
    }
  };

  return (
    <form onSubmit={handleSubmit}>
      <div>
        <label>Name:</label>
        <input type="text" value={name} onChange={(e) =>
            setName(e.target.value)} required />
      </div>
      <div>
        <label>Email:</label>
        <input type="email" value={email} onChange={(e) =>
            setEmail(e.target.value)} required />
      </div>
      <div>
        <label>Consent:</label>
        <input type="checkbox" checked={consent} onChange={(e) =>
            setConsent(e.target.checked)} />
        {consentText}
      </div>
      <div>
        <label>I confirm that I am of legal age:</label>
        <input type="checkbox" checked={isAdult} onChange={(e) =>
            setIsAdult(e.target.checked)} required />
      </div>
      <button type="submit">Submit</button>
    </form>
  );
}

export default ConsentForm;
```

Explanation: This updated form ensures that users confirm their age before submitting consent.

This is a necessary step to comply with legal requirements for processing the personal data of children and adolescents. If the user does not confirm they are of legal age, the form submission is blocked, and a warning is displayed.

Compliance with LGPD: This solution guarantees that data processing activities involving children and adolescents are conducted transparently and with specific consent from parents or legal guardians. Additionally, the form's accessible language ensures that the consent process is easy to understand for all users.

—

C-06: Does the system inform the data subject about changes in purpose and consent updates, allowing the data subject to revoke consent if they disagree with the changes?

Updating the Consent Interface

To address this requirement, the consent form component from item C-04 can be updated to notify the data subject of any changes in the purpose of data processing and the need for renewed consent. Additionally, the interface must allow the revocation of consent if the data subject disagrees with the updates.

This update ensures compliance with the General Data Protection Law (LGPD) and reinforces the principles of transparency and respect for the data subject's autonomy.

—

C-07: Does the system provide a consent declaration in an intelligible and easily accessible manner, without abusive terms?

Intelligible and Accessible Consent Declaration

The consent declaration must be written in clear and straightforward language to ensure all data subjects fully understand the information provided. The declaration must outline:

- How the data will be used.
- With whom it will be shared.
- The security measures in place to protect personal information.

The consent declaration must avoid technical jargon or abusive clauses and should uphold the data subject's rights. It should also foster transparency and trust between the controller and the data subject by clearly explaining:

- The purposes of data processing.
- The data subject's rights, including the ability to revoke consent.

By adhering to these principles, the consent declaration meets legal requirements and promotes an ethical data processing relationship.

—

C-08: Does the system inform the data subject about all their rights in the consent declaration?

Consent Declaration for the Processing of Personal Data

Dear Data Subject,

This Consent Declaration aims to inform and obtain your consent for the processing of your personal data in accordance with the General Data Protection Law (LGPD - Law No. 13,709/2018). Below, we describe in clear and accessible terms how your data will be used and your rights as a data subject.

1. Collection of Personal Data The personal data collected may include, but is not limited to: name, address, email, phone number, CPF, banking information, and other necessary details for the provision of our services.

2. Purpose of Data Processing The collected data will be used for the following purposes:

- Describe specific purposes, such as: service provision, communications, compliance with legal obligations, etc.

3. Data Sharing Your data may be shared with:

- List recipients, such as: business partners, service providers, competent authorities, etc.

4. Rights of the Data Subject Under the LGPD, you have the following rights regarding your personal data:

- **Confirmation of Processing:** The right to know if your data is being processed.
- **Access to Data:** The right to access your personal data processed by us.
- **Correction of Incomplete, Inaccurate, or Outdated Data:** The right to request the correction of your data.
- **Anonymization, Blocking, or Deletion:** The right to request the anonymization, blocking, or deletion of data that is unnecessary, excessive, or not compliant with the LGPD.
- **Data Portability:** The right to receive your data in a structured and interoperable format.
- **Deletion of Data Processed with Consent:** The right to request the deletion of data processed based on your consent, except as provided by law.
- **Information on Data Sharing:** The right to know which public and private entities your data is shared with.
- **Information on the Option to Not Consent:** The right to be informed about the possibility of not providing consent and the consequences of this decision.
- **Revocation of Consent:** The right to revoke consent at any time through an explicit request.

5. Data Security We adopt appropriate technical and organizational security measures to protect your personal data from unauthorized access, loss, destruction, or alteration.

6. Contact for Exercising Rights To exercise any of your rights or if you have questions about the processing of your personal data, please contact us at: [`youremail@domain.com`].

7. Changes to this Consent Declaration We reserve the right to update this Consent Declaration periodically. Any changes will be communicated to you through our usual communication channels.

By clicking the button below, you agree to the processing of your personal data as described above.

—

E.3 User Rights Templates

D-01: Does the system store personal data in a format that facilitates access for the data subject?

Database Structure: Ensure that the database structure allows easy retrieval of personal data for the data subject. For example, create a dedicated table to store consent information and related personal data.

API Endpoints for Personal Data Access: Implement API endpoints to enable the data subject to access, update, and delete their personal data.

- **Retrieve Personal Data:** Create an endpoint to allow users to view their personal data stored in the system.
- **Update Personal Data:** Create an endpoint to update personal data, enabling the data subject to correct or modify their information as needed.

User Interface: Develop an intuitive frontend interface for data subjects to view and manage their personal data.

- **Form for Viewing and Updating:** Provide a frontend form that allows data subjects to view their personal information and make updates.

Data Export: Implement a feature enabling the data subject to export their personal data in a standard format, such as JSON or CSV, to facilitate portability.

- **Export Endpoint:** Create an API endpoint to export the data subject's personal data in JSON or CSV format.
- **Export Interface:** Develop a frontend interface for users to request data exports and download the resulting file.

Notifications and Updates: Implement a notification system to inform the data subject of any changes in the purpose of their data processing and to request renewed consent if necessary.

- **Sending Notifications:** Establish a mechanism for sending notifications via email or other appropriate means.
- **Interface for Responding to Notifications:** Create a user interface where the data subject can view notifications and provide updated consent or revoke existing consent.

—

D-02: Does the system provide data subjects with a way to register complaints regarding the protection and processing of their personal data?

This requirement can be fulfilled by implementing the suggestion from item **T-09** (E.1), making the Data Protection Officer (DPO) or data processing contact available in the privacy policy or on a dedicated complaints page.

—

D-03: Does the system provide a full electronic copy of personal data to the data subject?

1. User Access Portal: Create a secure portal where users can access their personal information. The portal must be secured with robust authentication methods, such as two-factor authentication (2FA).

Features:

- **Data Access:** Allow users to view all personal information collected and stored.
- **Data Update:** Provide options for users to update their personal information directly within the portal.
- **Data Deletion:** Offer functionality for users to request the deletion of their personal data.

2. Authentication and Security:

- **Two-Factor Authentication (2FA):** Require an additional layer of authentication for portal access.
- **Data Encryption:** Ensure that all personal data is encrypted both at rest and in transit.
- **Access Logs:** Maintain logs of all user actions on their personal data, including viewing, editing, and deletion.

3. Intuitive User Interface:

- **Dashboard:** Create a dashboard summarizing personal data and available actions.
- **Edit Forms:** Provide simple forms for data updates.
- **Delete Button:** Include a clear, visible button for requesting data deletion, with double confirmation to avoid accidental actions.

4. Notifications and Confirmations:

- **Email Notifications:** Send email confirmations when data is accessed, edited, or deleted.
- **Request Status:** Inform users about the status of their data deletion requests, including processing steps and final confirmation.

—

D-04: Does the system allow the data subject to update their personal data?

Implement the features listed in **D-03** (E.3) to enable data updates.

—

D-05: Does the system use only relevant and adequate data for the purpose?

To ensure that the system uses only data that is relevant and adequate for its intended purpose, it is essential to follow a set of practices and procedures that ensure compliance with the General Data Protection Law (LGPD). Below are the guidelines for verifying the relevance and adequacy of the data collected and used by the system:

1. **Purpose Identification:**
   - Document the specific purposes for each data set.
   - Ensure that all individuals involved in data processing understand these purposes.
2. **Data Mapping:**
   - Create an inventory of data that includes all types of personal data collected, their sources, and the processes in which they are used.
   - Identify and categorize the data according to its relevance and adequacy to the established purposes.
3. **Data Minimization:**
   - Review forms and data collection processes to eliminate any data that is not essential for the declared purpose.
   - Implement controls to prevent the collection of unnecessary data.
4. **Regular Updates:**
   - Conduct periodic audits to review the relevance of the data collected in relation to the established purposes.
   - Update data collection and processing practices as necessary to reflect changes in purposes or the context of data use.
5. **Awareness:**
   - Provide regular training on the LGPD and data minimization practices to all employees involved in personal data processing.
   - Develop educational materials, such as manuals and best practice guides, to reinforce these concepts.
6. **Consent and Transparency:**
   - Provide clear and accessible privacy policies that explain in detail the purpose of data collection.
   - Obtain explicit consent from data subjects before collecting personal information, and allow users to easily review and revoke their consent.
7. **Documentation and Recordkeeping:**

- Document the justifications for collecting each type of personal data, demonstrating its relevance and adequacy to the purpose.
- Maintain records of audits, reviews, and training sessions conducted, as well as actions taken in response to findings from these activities.

—

D-06: Does the system allow data portability to another controller upon the data subject's request?

Personal data must be stored in an accessible and machine-readable format, ensuring that all information can be easily exported at any time. This is essential to meet requests from data subjects who wish to exercise their right to data portability, as stipulated by the General Data Protection Law (LGPD).

In addition to facilitating the transfer of information between different systems and platforms, this storage format ensures the integrity and usability of the data, allowing it to be interpreted and reused without loss of quality or meaning.

Adopting machine-readable formats, such as JSON, XML, or CSV, contributes to efficiency in internal data management processes and system interoperability. This approach meets both legal requirements and user expectations for transparency and control over their personal information.

—

D-07: Does the system delete personal data upon the data subject's request?

Implement features outlined in **D-03** (E.3) for data deletion requests.

—

D-08: Does the system delete the data subject's personal data after the end of its processing?

It is imperative that the data subject's personal data be deleted immediately after fulfilling the purpose for which it was collected, strictly adhering to the retention period established by the organization's data retention policy.

This procedure not only ensures compliance with the General Data Protection Law (LGPD) but also reinforces the organization's commitment to privacy and the security of user information. Proper deletion of data minimizes the risks of unauthorized access and misuse of information, as well as preserves the trust of data subjects by demonstrating that their data is not retained indefinitely or used for unauthorized purposes.

Implementing an automated and auditable process for data deletion can help ensure that this practice is carried out consistently and efficiently, aligning with best practices in data governance and privacy protection.

—

D-09: Does the system provide information about public and private entities in case of data sharing?

In cases of personal data sharing with other entities, the system must record information about the entities involved and the sharing operations performed.

This is necessary to enable future legal verifications and to ensure that these records are available upon request.

—

D-10: Does the system inform the data subject about the possibility of not providing consent and the consequences in case of refusal?

In the Consent Form, it is essential to provide the data subject with a clear option to refuse the processing of their personal information, transparently detailing the consequences of this decision.

This approach ensures that consent is truly informed and voluntary, aligned with the principles of the General Data Protection Law (LGPD). The form should clearly explain how refusal might impact the provision of services or access to certain functionalities offered by the organization. For example, refusal may result in limitations on the use of certain services or system features, and these implications should be clearly outlined to allow the data subject to make an informed decision.

Providing this information in a complete and understandable manner strengthens user trust in the organization, demonstrating a commitment to transparency and respect for the rights of data subjects.

—

D-11: Does the system inform the data subject when data processing is a condition for providing a product, service, or exercising a right?

Example of a message regarding the necessity of data collection for service provision:

Dear User,

We inform you that, to provide the requested product/service or to enable the exercise of certain rights, it is necessary to process your personal data.

This processing is essential for us to fulfill our obligations and ensure the quality and security of the services offered. By proceeding with this request, you acknowledge and agree to the collection and use of your personal data as described in our Privacy Policy. If you have any questions or need further information, we are available to assist you.

Sincerely,

—

D-12: Does the system allow data subjects to object to data processing easily?

It is essential to implement a mechanism that allows data subjects to withdraw their consent at any time in a simple and accessible manner.

This mechanism must be clearly available and easy to use, ensuring that the data subject can exercise their right without obstacles. When consent is withdrawn, the system must immediately cease the processing of the data subject's personal information, except in cases where another legal basis justifies the continuation of the processing.

Additionally, it is important to inform the data subject about the consequences of withdrawing consent, such as the possibility of no longer being able to access certain services or products that depend on the processing of their data.

The withdrawal of consent must be accompanied by a confirmation to the data subject, ensuring transparency and trust in the personal data management process.

—

D-13: Does the system inform the data subject of the reasons for not immediately exercising their rights?

When it is not possible to immediately execute an operation requested by the data subject, it is essential that the organization provides a clear and detailed response to the requester.

This response should address two possible situations:

First, if the organization is not the data processing agent responsible for the data, it must communicate this information to the data subject and, whenever possible, indicate the correct data processing agent so the request can be appropriately redirected.

Second, if there are factual or legal reasons that prevent the immediate adoption of the requested operation, the organization must transparently explain these reasons, detailing the specific motives that render the immediate execution of the request impossible.

This procedure not only ensures compliance with current legislation but also demonstrates the organization's commitment to transparency and open communication, reinforcing the data subject's trust in the management of their personal data.

—

D-14: Does the system inform the data subject when a decision has been made based on automated processing, including those aimed at creating their personal profile?

The mentioned item indicates that the system must notify the data subject whenever a decision is made automatically, without human intervention, based on the processing of their personal data. This includes decisions involving the creation of personal profiles, such as behavior analyses, preferences, or any other information that can be used to create a detailed profile of the data subject.

For example, if a system uses algorithms to evaluate a user's eligibility for a loan or to personalize product offers based on browsing behavior and purchase history, these decisions are automated. The system must, therefore, inform the data subject that such decisions were based on the automated processing of their data.

This transparency is essential for the data subject to understand how and why certain decisions were made and to ensure they have the opportunity to contest or request more information about the automated decision-making process, if necessary. This procedure complies with the principles of the General Data Protection Law (LGPD), which aims to protect the rights of data subjects concerning the automated processing of their personal information.

—

D-15: Does the system provide the option for the data subject to contest or request a review of the automated decision?

This item means that the system must offer data subjects the possibility to challenge or request a review of decisions made automatically, without human intervention.

When a system makes decisions based on algorithms or other forms of automated data processing, these decisions can significantly impact the data subject. Examples of such decisions may include credit approval or rejection, personalized offers, or any other action based on automated analyses of personal data.

To protect the rights of data subjects, it is important that they have the option to:

Contest the Decision: The data subject can disagree with the automated decision and present arguments or evidence to justify their contestation.

Request Human Review: The data subject can request that the automated decision be reviewed by a person, who will take into account individual circumstances and perform a more detailed and personalized analysis.

These options ensure that data subjects are not adversely affected by potentially unfair or erroneous automated decisions and provide an additional level of control over how their personal data is used. This practice complies with the principles of transparency, fairness, and accountability promoted by the General Data Protection Law (LGPD).

—

E.4 Data Security Templates

S-01: Does the system process data securely, including protection against unauthorized access?

To ensure that the system processes data securely, including protection against unauthorized access, it is essential to implement a series of practices and measures. The key points are highlighted below:

1. Data Encryption

- **Encryption in Transit:** Use protocols such as TLS (Transport Layer Security) to protect data during transmission between systems and devices.
- **Encryption at Rest:** Store sensitive data using robust algorithms such as AES (Advanced Encryption Standard).

2. Access Control

- **Strong Authentication:** Implement multi-factor authentication (MFA) to ensure that only authorized users can access the system.
- **Role-Based Access Control (RBAC):** Use a role-based access management model to manage permissions in a granular way.
- **Principle of Least Privilege:** Grant only the permissions necessary for users to perform their tasks.

3. Monitoring and Auditing

- **Log Records:** Maintain detailed logs of all system activities, including access attempts and data modifications.
- **Continuous Monitoring:** Use monitoring tools to detect and respond to suspicious activities in real time.
- **Regular Audits:** Conduct periodic audits to identify and address vulnerabilities.

4. Network Security

- **Firewall:** Configure firewalls to protect the network against unauthorized access and external attacks.
- **Network Segmentation:** Separate internal and external networks, and isolate critical system segments to limit the spread of attacks.

5. Vulnerability Management

- **Updates and Patches:** Keep software updated with the latest security fixes.
- **Penetration Testing:** Conduct regular penetration tests to identify and mitigate vulnerabilities.

6. Training and Awareness

- **Security Training:** Provide regular training to employees on data protection and best security practices.
- **Attack Simulations:** Conduct simulations to prepare the team to respond to security incidents.

7. Incident Response Plan

- **Plan Development:** Develop an incident response plan that includes procedures for detection, containment, eradication, and recovery.
- **Response Team:** Maintain a dedicated team with defined responsibilities to handle incidents.

8. Data Backup and Recovery

- **Regular Backups:** Perform regular backups of data, storing them securely in locations separate from the main environment.
- **Recovery Testing:** Test recovery procedures to ensure quick restoration in case of an incident.

Implementing these measures ensures that the system processes data securely, preventing unauthorized access and mitigating other risks to privacy and information security.

—

S-02: Does the system comply with the regulations for transferring personal data to international countries, ensuring an adequate level of personal data protection as per LGPD?

To ensure that the system complies with the regulations for transferring personal data to international countries under the LGPD, several steps and safeguards must be implemented:

1. Verification of Adequate Data Protection Level

- Verify if the recipient country offers an adequate level of data protection as determined by the Brazilian National Data Protection Authority (ANPD).
- If the country lacks adequate protection, adopt standard contractual clauses approved by the ANPD or draft specific agreements with additional guarantees.

2. Data Protection Impact Assessment (DPIA)

- Conduct a DPIA to identify and mitigate risks associated with international data transfers.
- Document the findings and the measures implemented to address identified risks.

3. Transparency and Consent

- Inform data subjects about the transfer, including the destination country and the protective measures in place.
- Obtain specific and informed consent from data subjects when there are no adequate protections or contractual guarantees.

4. Technical and Organizational Measures

- Implement robust encryption during data transfer to protect information from unauthorized access.
- Apply strict access controls to ensure that only authorized personnel can handle the transferred data.
- Monitor transfers continuously to detect and address potential vulnerabilities or breaches.

5. Documentation and Record-Keeping

- Maintain detailed records of all international transfers, including the legal justifications and the protection measures implemented.
- Ensure the availability of these records for audits or investigations by relevant authorities.

6. Global Cooperation and Best Practices

- Collaborate with international authorities and organizations to ensure alignment with global data protection standards.
- Participate in global forums on data protection to stay informed about new regulations and best practices.

By adopting these measures, the system ensures a legally compliant, secure, and transparent framework for the international transfer of personal data.

—

S-03: Does the system inform data subjects about personal data transfers to international countries?

The following text should be included in the Privacy Policy and Consent Terms:

To ensure compliance with the General Data Protection Law (LGPD), we inform that the personal data collected may be transferred to international countries when necessary for the execution of our activities and services. These transfers will be carried out in strict accordance with the principles and requirements established by the LGPD, always ensuring the protection and security of personal data. Data subjects will be informed in advance about such transfers, the destination countries, and the security measures adopted to protect their personal data. By providing their consent, the data subject expressly agrees to the international transfer of their data under the terms described.

—

S-04: Does the system use mechanisms to prevent data damage, destruction, or loss?

To ensure compliance with the requirement "Does the system use mechanisms to prevent data damage, destruction, or loss?" the following scripts can be used to implement prevention mechanisms. These scripts encompass best practices, including regular backups, data encryption, access control, and intrusion detection.

1. Regular Backup

A script to automate regular data backups. This can be scheduled for daily execution using `cron` on Linux.

```
#!/bin/bash

# Directory to be backed up
SOURCE_DIR="/path/to/source/directory"
# Backup destination directory
BACKUP_DIR="/path/to/backup/directory"
# Backup file name with timestamp
BACKUP_FILE="backup_$(date +'%Y%m%d%H%M%S').tar.gz"

# Create backup
tar -czf $BACKUP_DIR/$BACKUP_FILE $SOURCE_DIR

# Remove older backups (retain the last 7)
find $BACKUP_DIR -type f -name "*.tar.gz" -mtime +7 -exec rm {} \;
```

2. Data Encryption

A script to encrypt sensitive files using `OpenSSL`. This ensures data is secure against unauthorized access.

```
#!/bin/bash

# Directory with files to be encrypted
DATA_DIR="/path/to/data/directory"
# Directory for encrypted files
ENCRYPTED_DIR="/path/to/encrypted/directory"
# Encryption password
PASSWORD="your_secure_password"

# Encrypt each file in the directory
for FILE in $DATA_DIR/*; do
    openssl enc -aes-256-cbc -salt -in $FILE -out $ENCRYPTED_DIR/$(basename $FILE).enc
        -pass pass:$PASSWORD
done
```

3. Access Control

A script to configure permissions for sensitive files and directories, ensuring only authorized users can access them.

```
#!/bin/bash

# Directory with sensitive data
SENSITIVE_DIR="/path/to/sensitive/directory"
# Authorized user
AUTHORIZED_USER="authorized_user"
# Authorized group
AUTHORIZED_GROUP="authorized_group"

# Set directory owner and group
chown -R $AUTHORIZED_USER:$AUTHORIZED_GROUP $SENSITIVE_DIR

# Set access permissions
chmod -R 750 $SENSITIVE_DIR
```

4. Intrusion Detection

A script to configure `fail2ban`, a tool that protects the system from unauthorized access attempts.

```
#!/bin/bash

# Install fail2ban
sudo apt-get update
sudo apt-get install fail2ban -y

# Configure fail2ban to protect SSH
cat <<EOT >> /etc/fail2ban/jail.local
```

```
[sshd]
enabled = true
port = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s
maxretry = 3
bantime = 3600
EOT

# Restart fail2ban to apply the configuration
sudo systemctl restart fail2ban
```

These scripts address key mechanisms to prevent data damage, destruction, or loss. It is crucial to review and adapt them to the specific needs of the system and infrastructure in use. Additionally, implementing these practices should be complemented by robust policies and procedures to ensure effective data security management.

—

S-05: Does the system use appropriate protection measures for sensitive personal data?

To ensure sensitive personal data is adequately protected in PostgreSQL, several measures can be implemented, including data encryption and access control. Below are examples of configuration scripts for these measures.

1. Data Encryption at Rest

To encrypt data at rest in PostgreSQL, use the ‘pgcrypto‘ extension. First, install the extension if it is not already installed:

```
CREATE EXTENSION IF NOT EXISTS pgcrypto;
```

Then, use encryption functions to store sensitive data. For example, to encrypt a credit card number field:

```
-- Create a table with an encrypted field
CREATE TABLE usuarios (
    id SERIAL PRIMARY KEY,
    nome VARCHAR(100),
    cartao_credito BYTEA
);

-- Insert data with encryption
INSERT INTO usuarios (nome, cartao_credito)
VALUES (’João Silva’, pgp_sym_encrypt(’1234-5678-9012-3456’, ’chave_secreta’));
```

```
-- Decrypt data
SELECT id, nome, pgp_sym_decrypt(cartao_credito, ’chave_secreta’) AS cartao
FROM usuarios;
```

2. Access Control

To implement proper access control, define roles and permissions. For example:

```
-- Create roles
CREATE ROLE auditor NOINHERIT;
CREATE ROLE administrador NOINHERIT;

-- Grant permissions
GRANT CONNECT ON DATABASE meu_banco_de_dados TO auditor;
GRANT SELECT ON ALL TABLES IN SCHEMA public TO auditor;

GRANT CONNECT ON DATABASE meu_banco_de_dados TO administrador;
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA public TO administrador;
```

To ensure only authorized users access sensitive data, define specific views or use Row Level Security (RLS):

```
-- Enable RLS on the table
ALTER TABLE usuarios ENABLE ROW LEVEL SECURITY;

-- Create policies
CREATE POLICY seletiva_acesso ON usuarios
    USING (current_user = ’administrador’);

-- Enforce row-level security
ALTER TABLE usuarios FORCE ROW LEVEL SECURITY;
```

3. Auditing

To audit access and data changes, use the ‘pgaudit‘ extension:

```
-- Install and configure pgaudit
CREATE EXTENSION IF NOT EXISTS pgaudit;

-- Configure in postgresql.conf
-- Add the following lines:
shared_preload_libraries = ’pgaudit’
pgaudit.log = ’all’

-- Reload PostgreSQL configuration
SELECT pg_reload_conf();
```

Summary

The scripts above cover essential measures for protecting sensitive personal data in PostgreSQL, including data encryption at rest, granular access control, and database operation auditing. These practices help ensure compliance with the LGPD and the protection of sensitive personal data.

—

S-06: Does the system adopt good privacy protection practices, such as privacy by design?

Applying the concept of Privacy by Design in system development involves integrating data protection and privacy principles from the beginning of the system creation process, rather than as an afterthought. Initially, it is essential to conduct a privacy analysis during the early stages of the project to identify which personal data will be collected, how it will be used, stored, and shared. This analysis should consider the risks associated with data processing and the necessary measures to mitigate them. This includes minimizing data collection, ensuring only the information strictly necessary for system functionality is collected, and implementing techniques such as anonymization and pseudonymization to protect individuals' identities.

During system development, it is crucial to incorporate features that ensure data security and privacy. This can be achieved through implementing robust access controls, encrypting data at rest and in transit, and establishing continuous audit and monitoring mechanisms. Additionally, the system should be designed to facilitate the fulfillment of data subjects' rights, such as the rights to access, rectify, delete, and port their personal data. This requires the creation of intuitive user interfaces and efficient administrative processes that allow individuals to exercise their rights easily and effectively.

Finally, fostering a culture of Privacy by Design throughout the organization is essential. This involves ongoing training for developers and other staff on best practices for privacy and data protection, as well as creating a governance framework to ensure compliance with the LGPD and other applicable regulations. The organization should conduct regular privacy impact assessments and be prepared to adjust its practices as needed to address new risks and challenges. By adopting a proactive and preventive approach, the organization not only protects individuals' personal data but also strengthens trust and reputation with its users and customers.

—

S-07: Does the system map personal data and keep it secure?

To effectively map personal data and ensure its security, the system must implement a detailed inventory of all personal data collected, stored, processed, and shared, categorizing it according to its sensitivity and intended use. This mapping should be continuously updated to reflect any changes in data processing activities. Additionally, the system should employ encryption techniques to safeguard data at rest and in transit, enforce strict access controls to ensure that only authorized personnel can access the data, and implement auditing and monitoring mechanisms to detect and respond to any security incidents. These measures ensure that personal data is protected against unauthorized access, loss, or breaches, in compliance with the requirements of the General Data Protection Law (LGPD).

—

S-08: Does the system ensure data confidentiality using appropriate technical measures?

To meet this requirement, it is essential to adopt a series of practices and technologies that safeguard personal data against unauthorized access:

- Implement strong encryption (e.g., AES-256) to protect data at rest and in transit.
- Use secure protocols, such as TLS, for the transmission of sensitive data over the internet.
- Employ multi-factor authentication (MFA) to add an extra layer of security to user authentication.
- Enforce strong password policies and periodic password renewals.
- Store passwords securely using safe hashing algorithms (e.g., bcrypt) with salting.
- Use continuous monitoring tools to detect and respond quickly to suspicious or unauthorized activities.
- Maintain detailed audit logs for all data access and modification operations.
- Rely on frameworks and libraries that adhere to security best practices and are regularly updated.
- Conduct regular training for employees on secure data handling practices and awareness of security threats.
- Establish clear procedures for responding to security incidents and data breaches.
- Configure firewalls and intrusion prevention systems (IPS) to protect the network and servers hosting the system.
- Ensure that all systems and software are updated with the latest security patches.
- Implement regular backup policies and store backups securely.
- Periodically test disaster recovery plans to ensure that data can be restored quickly in case of incidents.

By implementing these measures, the system ensures data confidentiality, mitigates risks, and complies with data protection regulations such as the LGPD.

—

S-09: Does the system ensure the integrity of personal data, preventing modifications?

To guarantee data integrity, the system can employ techniques such as checksums or hash functions like SHA-256 to generate unique values that represent the original state of the data. Each time the data is stored or transmitted, the system should compute a new hash and compare it with the previously stored hash. If the hash values do not match, this indicates that the data has been altered without authorization or was corrupted during transmission.

—

S-10: Does the system maintain compliance audit logs and provide information to data subjects upon request?

The system must include audit functionalities that record all activities related to the processing of personal data, including access, modifications, sharing, and deletions. These records should be securely maintained and accessible only to authorized personnel to ensure the integrity and confidentiality of the information. Additionally, the system must be capable of generating detailed compliance reports that can be easily made available to data subjects upon request. This ensures transparency and provides data subjects with a clear understanding of how their data is being managed. Implementing a self-service portal can facilitate access to such information, enabling data subjects to make requests and receive responses quickly and efficiently.

—

S-11: Does the organization have a remediation plan for privacy and security incidents?

Draft of Privacy and Security Incident Remediation Plan

1. Incident Identification

- Continuous system monitoring to detect suspicious activities.
- Clear definition of criteria for what constitutes a privacy and security incident.

2. Immediate Containment

- Isolation of affected systems or components to prevent incident spread.
- Implementation of temporary measures to limit immediate impact.

3. Initial Assessment

- Quick analysis to determine the nature and extent of the incident.
- Identification of compromised personal data and attack vectors.

4. Notification

- Immediate communication to internal stakeholders, such as IT teams and the Data Protection Officer (DPO).
- Notification to affected data subjects, as required by the LGPD.
- Initial reporting to regulatory authorities, if necessary.

5. Detailed Investigation

- Conducting a thorough investigation to understand the root cause of the incident.
- Documenting all steps taken during the investigation.

6. Correction and Mitigation

- Implementation of permanent fixes to address identified vulnerabilities.

- Application of additional measures to prevent recurrence of the incident.
- Updating security policies and procedures as necessary.

7. Recovery

- Restoration of affected systems and data to their normal operational state.
- Assurance that all systems are secure and functioning correctly.

8. Review and Learning

- Conducting a post-incident review to evaluate the response and identify improvements.
- Recording lessons learned and adjusting the incident remediation plan.

9. Final Reporting

- Compilation of a detailed incident report, including causes, actions taken, and future prevention measures.
- Sharing the report with relevant stakeholders and regulatory authorities, as necessary.

10. Continuous Training

- Ongoing training of employees on security and privacy policies.
- Regular updates to the incident remediation plan based on new threats and vulnerabilities.

—

S-12: Does the system have certifications or seals to demonstrate compliance with personal data protection regulations?

To comply with the requirement that the system possess certifications or seals demonstrating adherence to personal data protection regulations, the organization should pursue recognized certifications such as ISO/IEC 27701, which specifies requirements and guidelines for a privacy information management system. Obtaining such certifications involves implementing rigorous policies and processes for personal data management, regular audits by independent third parties, and continuous adherence to best practices in security and privacy. Displaying certification seals within the system and communications with users not only demonstrates the organization's commitment to regulatory compliance but also enhances user trust by ensuring that their information is handled according to the highest standards of data protection.

—

S-13: Does the system implement a process for registration, deactivation, and provisioning for access control?

To ensure effective access control, the system must implement a secure registration process capable of validating and reliably storing user information. This process should use unique credentials for each user, ensuring that each account is securely identifiable and traceable. Registration validation should incorporate robust authentication methods, such as multi-factor authentication (MFA), to provide an additional layer of security. Secure storage of credentials should involve cryptographic hashing functions to transform passwords into irreversible character sequences and salting practices to add random data to passwords before hashing, further complicating brute force or dictionary attacks.

In addition to secure registration, automated or semi-automated processes for removing users whose access is no longer required are essential. These processes should integrate with the user's lifecycle within the system, from account creation to deactivation and removal. For example, when a user's access is no longer needed, their credentials should be immediately revoked and their accounts disabled or removed. Implementing account expiration policies and conducting regular audits help identify and remove inactive or obsolete accounts, minimizing the risk of unauthorized access. Automating these processes not only improves efficiency but also ensures consistent application of security policies.

Finally, managing access to system resources should be based on a role-based access control (RBAC) model. This model involves clearly defining roles and the permissions associated with each, aligning them with the users' responsibilities within the organization. Each user should be assigned one or more roles, with permissions specifying the resources they can access and the actions they can perform. Access control policies must be rigorously enforced to ensure users have only the permissions necessary for their roles. Periodic reviews of role assignments and permissions are crucial for maintaining security, adapting permissions to evolving user roles, and addressing new threats or vulnerabilities.

—

S-14: Does the system have a formal process for user registration and deactivation in systems that process personal data?

To effectively control access to systems handling personal data, it is crucial to implement a secure user registration and deactivation process. This includes creating a registration system that robustly validates user identity and securely stores user information. Additionally, upon user deactivation, the system must ensure that all permissions are immediately revoked and that the user's data is handled in accordance with established deletion policies, guaranteeing no unauthorized access or improper retention of personal data.

Strong password and permission policies are essential to ensure system security. These policies should include requirements for complex passwords, periodic password renewal, and the implementation of multi-factor authentication (MFA) to provide an additional layer of security. Permissions should be managed based on the principle of least privilege, where users are granted only the access necessary to perform their specific functions. This approach helps minimize potential damage in the event of security breaches and ensures that sensitive information is accessible only to authorized personnel.

Regular auditing and security training are critical components for maintaining system security. Auditing involves continuous tracking of user activities to detect and respond to suspicious or unauthorized actions. This may include reviewing access logs, monitoring anomalous behaviors, and conducting periodic compliance audits. Additionally, regular security training for all staff ensures they are aware of best practices and their responsibilities when handling personal data. Finally, the software must consistently comply with data privacy regulations, such as the General Data Protection Law (LGPD), to ensure that all data processing practices align with current legal and regulatory requirements.

—

S-15: Does the system have a formal process for granting or revoking access rights?

To address the granting or revoking of access rights in a system, it is highly recommended to implement an Identity and Access Management (IAM) solution. This type of solution provides a comprehensive set of functionalities that facilitate the secure and efficient management of user identities and their respective access rights to system resources.

IAM offers identity provisioning, which is the process of creating, updating, and removing user identities within the system. This ensures that only authorized users can access the system from the outset and that their permissions are adjusted as their roles change. Multi-factor authentication (MFA) is a crucial feature, adding an extra layer of security by requiring users to confirm their identity through two or more verification methods, such as a password and a code sent to a mobile device.

Another essential feature is permissions and role management, which enables assigning access rights based on specific organizational roles. This ensures that users have only the permissions necessary to perform their tasks, minimizing the risk of unauthorized access to sensitive data. IAM's password management simplifies the creation and enforcement of secure password policies, including complexity requirements and password change frequencies.

Additionally, IAM offers access audit and reporting capabilities, providing visibility into who accessed what and when, which is critical for detecting and responding to suspicious activities. Lastly, deprovisioning ensures the revocation of identities and permissions for users who no longer need access, safeguarding against unauthorized access by former employees or temporary users after their departure.

In summary, an IAM system significantly enhances information security and operational efficiency, providing strict control over access to system resources while ensuring compliance with data protection policies and regulations.

—

S-16: Does the system maintain an accurate and updated record of authorized users accessing information systems or personal data contained therein?

To implement an accurate and updated record of authorized users accessing information systems or personal data using PostgreSQL, the following steps can be followed:

1. User Table Creation

Create a table to store user information, including details about their permissions and authorization status.

```
CREATE TABLE usuarios (
    id SERIAL PRIMARY KEY,
    nome VARCHAR(100) NOT NULL,
    email VARCHAR(100) UNIQUE NOT NULL,
    data_autorizacao TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    status_autorizacao BOOLEAN DEFAULT TRUE,
    data_revogacao TIMESTAMP,
    motivo_revogacao TEXT
);
```

2. Registering a New User

Insert a new record for each user authorized to access the system.

```
INSERT INTO usuarios (nome, email)
VALUES ('João Silva', 'joao.silva@example.com');
```

3. Updating Authorization Status

To revoke user access, update the authorization status and log the date and reason for revocation.

```
UPDATE usuarios
SET status_autorizacao = FALSE,
    data_revogacao = CURRENT_TIMESTAMP,
    motivo_revogacao = 'Acesso revogado devido à saída da empresa'
WHERE email = 'joao.silva@example.com';
```

4. Querying Authorized Users

Retrieve a list of all users currently authorized to access the system.

```
SELECT * FROM usuarios
WHERE status_autorizacao = TRUE;
```

5. Audit and Logging

Create an audit table to record all changes in user authorization status.

```
CREATE TABLE auditoria_autorizacao (
    id SERIAL PRIMARY KEY,
    usuario_id INT REFERENCES usuarios(id),
    acao VARCHAR(50),
    data_acao TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    detalhes TEXT
);
```

6. Logging Actions in the Audit Table

Insert records into the audit table whenever there is a change in user authorization status.

```
INSERT INTO auditoria_autorizacao (usuario_id, acao, detalhes)
VALUES (1, 'Revogação de Acesso', 'Acesso revogado devido à saída da empresa');
```

7. Trigger Implementation

Create triggers to automate logging changes into the audit table.

```
CREATE OR REPLACE FUNCTION registrar_auditoria()
RETURNS TRIGGER AS $$
BEGIN
    IF (TG_OP = 'UPDATE') THEN
        IF (NEW.status_autorizacao = FALSE AND OLD.status_autorizacao = TRUE)
        THEN
            INSERT INTO auditoria_autorizacao (usuario_id, acao, detalhes)
            VALUES (NEW.id, 'Revogação de Acesso', NEW.motivo_revogacao);
        ELSIF (NEW.status_autorizacao = TRUE AND OLD.status_autorizacao = FALSE)
        THEN
            INSERT INTO auditoria_autorizacao (usuario_id, acao, detalhes)
            VALUES (NEW.id, 'Restabelecimento de Acesso', 'Acesso restabelecido');
        END IF;
    END IF;
    RETURN NEW;
END;
$$ LANGUAGE plpgsql;

CREATE TRIGGER trigger_registrar_auditoria
AFTER UPDATE ON usuarios
FOR EACH ROW
EXECUTE FUNCTION registrar_auditoria();
```

By following these steps, the system ensures accurate tracking of authorized users and their access status, thereby strengthening compliance with data protection regulations like LGPD and improving overall system security.

—

S-17: Does the system implement the protection of personal data in transit (SSL) and at rest?

To ensure the protection of personal data both in transit and at rest, robust encryption strategies are essential. The use of SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security) is critical for safeguarding the integrity and privacy of data transmitted over the internet. SSL/TLS encrypts the data exchanged between the client and server, preventing interception or tampering by unauthorized third parties. This is particularly crucial for sensitive information such as personal data, passwords, and financial transactions, protecting against man-in-the-middle attacks.

Beyond data in transit, ensuring the security of stored data is equally important. The following approaches can be implemented:

1. Disk-Level Encryption

Disk-level encryption, such as BitLocker for Windows or FileVault for macOS, encrypts the entire storage drive, ensuring that the data remains inaccessible if the physical disk is removed or accessed without proper authorization. This method effectively protects entire storage devices against unauthorized access.

2. Database-Level Encryption

Database-level encryption, such as Transparent Data Encryption (TDE) available in databases like Oracle, provides encryption for data stored within the database itself. TDE ensures that sensitive information is only accessible to authorized users with the appropriate decryption keys. This approach adds a layer of security specifically tailored for large-scale database systems.

3. Application-Level Encryption

Application-level encryption involves encrypting data within the application before storing it. This provides flexibility for developers to choose which data to encrypt based on its sensitivity and use case. For instance, personally identifiable information (PII) or credit card numbers can be encrypted at the application level before being saved to the database, ensuring protection even if the underlying database or storage system is compromised.

Implementation Example: SSL/TLS and Data Encryption

```
# Enabling SSL/TLS in Apache (example for web servers)
<VirtualHost *:443>
    SSLEngine on
    SSLCertificateFile /path/to/certificate.crt
    SSLCertificateKeyFile /path/to/private.key
    SSLCertificateChainFile /path/to/chain.pem
</VirtualHost>

# Using AES-256 for application-level encryption in Python
from cryptography.fernet import Fernet

# Generate and store a secure key
key = Fernet.generate_key()
cipher = Fernet(key)

# Encrypt data
plaintext = b"Sensitive data"
ciphertext = cipher.encrypt(plaintext)

# Decrypt data
decrypted_data = cipher.decrypt(ciphertext)
```

Conclusion

When implemented together, SSL/TLS for data in transit and encryption strategies for stored data create a comprehensive defense mechanism. These practices protect sensitive information from unauthorized access, ensuring compliance with data protection regulations like LGPD and building user trust through robust security measures.

—

E.5 Controller Responsibilities Templates

R-01: Does the organization designate a Data Protection Officer (DPO) responsible for the processing of personal data?

The organization must appoint a Data Protection Officer (DPO), who can be an individual or a legal entity, to serve as the primary point of contact between the data controller, data subjects, and the National Data Protection Authority (ANPD). The DPO is responsible for ensuring that the organization's data processing practices comply with the General Data Protection Law (LGPD).

The ANPD has the authority to establish complementary regulations regarding the activities of the DPO and may even waive the requirement for such a designation, depending on the organization's size and nature. The DPO's role is fundamental in promoting transparency and effectiveness in personal data protection, while also facilitating communication between all stakeholders involved.

—

R-02: Does the organization publicly disclose, clearly and objectively, the identity and contact information of the Data Protection Officer (DPO)?

This information must be clearly stated in both the Privacy Policy and the Consent Form, ensuring that data subjects and the National Data Protection Authority can easily and comprehensibly access all relevant details. The language used should be simple and accessible, avoiding technical jargon that could hinder understanding.

Additionally, these documents should be easily located in both digital and physical formats, promoting transparency and trust in the handling of personal data. Clear presentation of this information is essential to ensure that data subjects are aware of their rights and the data protection practices adopted by the organization. It also demonstrates compliance with the General Data Protection Law (LGPD).

—

R-03: Does the organization notify the national authority and the data subjects of a security incident that may cause significant risk or harm to the subjects, within the deadlines established by the authorities?

In the event of a security incident, it is essential to promptly notify both the data subjects and the National Data Protection Authority (ANPD). The ANPD recommends that this notification be made within 2 business days from the moment the incident is identified, even if it is still under investigation and not fully confirmed. In such cases, a preliminary notification should be sent to avoid any violation of the General Data Protection Law (LGPD).

The content of this notification must at least meet the requirements of §1 of Article 48 of the LGPD and can also be supplemented according to the form available on the ANPD website (<https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>). This swift and efficient action is crucial to ensure transparency, compliance with legal requirements, and to minimize potential harm to the data subjects involved.

—

R-04: Does the organization conduct a Data Protection Impact Assessment (DPIA) when processing results in high risks to the rights and freedoms of data subjects?

Below is an example of a structured Data Protection Impact Assessment (DPIA) document:

1. Introduction

Objective: This document aims to conduct a Data Protection Impact Assessment as required by the General Data Protection Law (LGPD) when data processing involves high risks to the rights and freedoms of data subjects. **Scope:** Define the data processing activities with high risk and detail the measures adopted to mitigate these risks.

2. Description of Data Processing

2.1. Processing Activities: - Detailed description of the data processing activities. - Identification of personal data collected, processed, stored, and shared.

2.2. Purpose of Processing: - Explanation of the specific purpose of the data processing. - Justification of the necessity and proportionality of the processing.

2.3. Legal Basis: - Indication of the legal basis supporting the processing, in accordance with the LGPD.

3. Risk Assessment

3.1. Identification of Risks: - Listing of potential risks to the data subjects' data protection. - Assessment of the severity and likelihood of each identified risk.

3.2. Impact on Data Subjects: - Description of the potential impact of the identified risks on the rights and freedoms of data subjects, considering aspects like privacy, discrimination, financial loss, and others.

4. Mitigation Measures

4.1. Technical and Organizational Measures: - Detailed description of the technical and organizational measures implemented to mitigate the identified risks. - Examples include encryption, anonymization, access controls, information security policies, training, among others.

4.2. Monitoring and Review: - Explanation of the continuous monitoring process and review of the implemented mitigation measures. - Definition of the review periodicity and identification of those responsible for its execution.

5. Consultation with the Data Protection Officer (DPO)

5.1. DPO Identification: - Identification of the Data Protection Officer responsible for conducting this assessment. - Record of consultations held with the DPO during the assessment process.

6. Conclusion

6.1. Results: - Presentation of the conclusions of the DPIA. - Determination of whether the risks have been adequately mitigated or if additional actions are required.

6.2. Final Report: - Generation of a final report documenting all steps of the assessment, including the description of processing activities, risk identification and evaluation, implemented mitigation measures, and consultations with the DPO.

Attachments: Additional documents and evidence supporting the assessment process.

Date: **Responsible:** **Approved by:**

—

R-05: Does the organization prepare a Data Protection Impact Report and make it available to the national authority upon request?

It is imperative that a Data Protection Impact Report is prepared and made available to the national authority when requested. This report must include, at a minimum:

- **Detailed Description of Data Types:** A clear and comprehensive overview of the types of data collected, processed, and stored by the organization.
- **Methodology Employed:** An explanation of the methodologies used for data collection and processing, ensuring transparency in the treatment processes.
- **Security Measures:** A thorough description of the strategies adopted to ensure the security and integrity of the data, including technical and organizational measures.
- **Controller's Analysis:** A detailed analysis by the data controller, addressing the effectiveness of the measures implemented, the safeguards established, and the mechanisms used to mitigate risks associated with the processing of personal data.

These components ensure compliance with the General Data Protection Law (LGPD) and demonstrate a commitment to protecting the rights of data subjects. The availability of such a report, when requested by the national authority, reinforces the organization's transparency and accountability in data protection practices.

—

R-06: Does the organization record the activities performed by the DPO for potential legal evidence?

The organization must maintain a detailed record of all activities carried out by the Data Protection Officer (DPO). These records should include:

- **Interactions:** Documentation of all interactions with data subjects, internal teams, and external stakeholders.
- **Decisions:** Records of decisions made regarding data protection policies, incident responses, and compliance strategies.
- **Compliance Measures:** Details of compliance measures implemented to align with data protection laws.
- **Training Activities:** Information on privacy and data protection training sessions conducted for employees.
- **Communications:** Logs of any correspondence with regulatory authorities and data subjects, including inquiries, incident notifications, and requests for information.

These records are critical for providing clear and robust evidence in the event of audits or investigations. They demonstrate compliance with the obligations and regulations established by the General Data Protection Law (LGPD), ensuring transparency and accountability in the organization's data protection practices.

—

R-07: Does the organization provide training for its employees on compliance with the LGPD?

The organization must implement ongoing training programs for its employees, focusing on compliance with the guidelines established by the General Data Protection Law (LGPD). These training sessions should cover a broad range of topics, including:

- **Fundamental Principles of LGPD:** Understanding the core principles and objectives of the law.
- **Roles and Responsibilities:** Individual and collective responsibilities in protecting personal data.
- **Best Practices:** Techniques and strategies to ensure the security and integrity of personal data.
- **Handling Requests and Incidents:** Correct procedures for responding to data privacy requests and managing security incidents.

Furthermore, it is essential that these training programs are regularly updated to reflect any changes in legislation or internal policies. This ensures that employees remain well-informed and fully equipped to maintain compliance with the LGPD, safeguarding the rights of data subjects and enhancing the organization's overall data protection posture.

—

F Research Participation Invitation

Dear Participant,

With the aim of supporting the evaluation of the compliance of computational systems with the LGPD, LGPD-Check is a checklist developed and improved to identify potential non-compliance issues and suggest necessary corrective measures. Additionally, we have developed templates to assist in meeting the checklist requirements.

In this context, you have been selected based on your profile, knowledge, and experience to evaluate the recommendations and templates provided by the checklist, with the purpose of addressing each identified non-compliance issue.

The checklist contains 61 items, organized into 47 mandatory items required by the LGPD law and 14 optional items consisting of recommendations and improvement opportunities. The items are grouped into five categories: Data Transparency, User Consent, User Rights, Data Security, and Controller Responsibilities.

This data collection will support the continuous improvement of LGPD-Check within the scope of a Master's research project. The estimated time for evaluating the LGPD-Check templates is 1 hour.

Study Procedure

The study will be conducted in four steps:

1. **Presentation of LGPD-Check** through the video call link:
   `https://meet.google.com/[omitted]`
2. **Filling Out the Informed Consent Form**
3. **Filling Out the Characterization Form**
4. **Evaluation of LGPD-Check Recommendations and Templates**
   Evaluation period: June 18-24, 2024
5. **Participation in a Focus Group Meeting**
   Scheduled for: June 25, 2024, at 09:00 (GMT-4)

Contact Information

We thank you in advance for your collaboration. If you have any questions or require any assistance while filling out the checklist, please feel free to contact me.

Sincerely,
Christiano Neitzke
UFMA / PPGCC

G Participant Instructions

Dear Participant,

We are pleased to welcome your involvement in our study on LGPD-Check. To proceed, we kindly ask you to access the following link:

`https://forms.gle/QNoaKxUQ9558qtpw9`

Please complete the Informed Consent Form (ICF), essential for your participation in the study, and the Characterization Form, which collects relevant information about you.

Additionally, individualized access to the online checklist spreadsheet has been provided, allowing you to verify system compliance and evaluate the recommendations and templates offered by the tool.

Important Deadlines

- Evaluation Deadline: **June 24, 2024**
- Focus Group Meeting: **June 25, 2024, at 09:00 (GMT-4)**

During the focus group meeting, we will identify the strengths and weaknesses of the templates and recommendations for each checklist item, discuss challenges encountered during application, and gather practical improvement suggestions.

Checklist Item Allocation

To ensure balanced checklist item distribution among participants, we have established the following assignment, with a minimum of 12 items per evaluator:

Evaluator	**Assigned Items**
I-01	From item T-01 to T-12
I-02	From item T-07 to C-04
I-03	From item T-13 to D-02
I-04	From item C-05 to D-08
I-05	From item D-03 to D-14
I-06	From item D-09 to S-05
I-07	From item D-15 to S-11
I-08	From item S-06 to S-17
I-09	From item S-12 to R-07
I-10	From item R-01 to R-07 and from T-01 to T-05

Checklist Completion Guidelines

While using the checklist, please remember to fill out the spreadsheet header fields, including:

- Inspection Start Date

- Inspection End Date
- Time Spent Completing the Checklist

To facilitate template evaluation, items from the same category have been kept within the same file, streamlining the analysis and evaluation process.

Presentation Recording

The LGPD-Check presentation recording can be accessed via the following link:

`https://drive.google.com/file/d/17tUGXReOmejncxPhv2gEQeFbm27gMSno/view`

Your collaboration is essential to the success of this research. We sincerely appreciate your participation and commitment to data protection.

Sincerely,
Christiano Neitzke
UFMA / PPGCC

H Agenda for the Focus Group Meeting

1. **Welcome and Introduction (3 minutes)**
   a) Greetings to the participants
   b) Introduction of the moderator and observer
   c) Brief description of the meeting's objectives
   d) Explanation of the focus group dynamics and the role of each participant
   e) Assurance of confidentiality and anonymity
2. **Introduction to LGPD-Check (5 minutes)**
   a) Overview of the LGPD-Check project
   b) Explanation of the checklist's objectives and its importance in LGPD compliance
   c) Description of the structure of the templates and their categories
3. **Discussion on Recommendations and Templates – Transparency of Data (15 minutes)**
   a) Presentation of items related to *Transparency of Data*
   b) Discussion prompts:
      i. Are the items clear and understandable?
      ii. Did you encounter any difficulties in interpreting the recommendations?
      iii. Suggestions for improvements?
4. **Discussion on Recommendations and Templates – User Consent (15 minutes)**
   a) Presentation of items related to *User Consent*
   b) Discussion prompts:
      i. Are the items adequate to ensure informed consent?
      ii. Are there recommendations that require further clarification?
      iii. Suggestions for improvements?
5. **Discussion on Recommendations and Templates – User Rights (15 minutes)**
   a) Presentation of items related to *User Rights*
   b) Discussion prompts:
      i. Do the items adequately address user rights?
      ii. Are the recommendations practical and applicable?
      iii. Suggestions for improvements?
6. **Discussion on Recommendations and Templates – Data Security (15 minutes)**
   a) Presentation of items related to *Data Security*
   b) Discussion prompts:
      i. Are the recommendations sufficient to ensure data security?

   ii. Are there recommendations requiring further elaboration?
   iii. Suggestions for improvements?

7. **Discussion on Recommendations and Templates – Controller Responsibilities (10 minutes)**
   a) Presentation of items related to *Controller Responsibilities*
   b) Discussion prompts:
      i. Are the responsibilities well-defined?
      ii. Are the recommendations practically applicable?
      iii. Suggestions for improvements?

8. **General Discussion and Final Feedback (10 minutes)**
   a) Open-ended questions for general feedback on the templates
   b) Solicitation of additional suggestions not covered during specific discussions
   c) Final remarks from participants

9. **Closing (2 minutes)**
   a) Acknowledgment of participants' contributions
   b) Provision of contact information for additional feedback or inquiries