RIPD Model: Data Protection Impact Report – LGPD

"Insert the title and subtitle here."

Disclaimer

The RIPD (Relatório de Impacto à Proteção de Dados), or Data Protection Impact Report under LGPD, is similar to the DPIA (Data Protection Impact Assessment) under GDPR. Both assess and describe risks in data processing activities that may affect individuals' rights and outline measures to ensure compliance with data protection laws. Despite differences in terminology and frameworks, their core objectives are aligned. Below, we outline the report components based on the requirements from the Compliance, Legal, and Information Security departments of SESI and SENAI São Paulo, Brazil, ensuring alignment with regulatory standards and internal policies.

Version Control

Data	Version	Description	Autor
01/12/2023	1.0 Draft	Draft model version	Hebert Silva
01/04/2024	1.1 First	First version revised	Hebert Silva

Table of Contents

1. Objective

Explain how the report aims to identify potential data privacy risks in data processing activities and outline measures to mitigate these risks, ensuring compliance with relevant data protection laws such as LGPD or GDPR. The Data Protection Impact Report aims to describe the personal data processing activities that may pose risks to civil liberties and fundamental rights, as well as the measures, safeguards, and risk mitigation mechanisms in place.

- **LGPD Reference**: Art. 5º, XVII.
- **Compliance**: The RIPD's objective addresses the need to describe data processing activities that may pose risks to data subjects, meeting the requirement of creating impact reports for data protection.
- **Example Scenario:** A company Industries, a manufacturing company, implements an RIPD to align HR data handling with LGPD requirements, focusing on minimizing risks of unauthorized access during payroll processing.

2. Identification of Data Processing Agents

List the main entities involved in data processing, including the data controller, operators (if applicable), and the data protection officer (DPO). Provide their contact information and responsibilities in the context of data protection.

- **LGPD Reference**: Art. 5º, VI and VII.
- **Compliance**: Identifies roles such as controllers and DPOs, fulfilling the requirement to clearly define the responsibilities of those handling personal data.
- **Example Scenario:** The Industries identifies the HR manager as the data controller, IT staff as operators managing data, and the DPO ensures compliance.

For each identified risk, the Probability of occurrence and the Severity—how much damage could be caused if the threat materializes—are defined. The following Table1 - will be used as a reference for classifying the probability and severity.

Table 1 – Risk Classification

	Impact	
Value	**Probability (Chance of the threat materializing)**	**Severity (Damage if it occurs)**
1	Low	Low
2	Medium	Medium
3	High	High
4	Very High	Very High

Probability is assessed based on the number of events of the same nature as the risk within a given period. Thus, for the processing of personal data related to the services under analysis in the RIPD, the risks can be classified as follows and presented as per Table 2 – Risk Assessment.

Table 2 - Risk Assessment

Item	Title of Risk	Probability	Severity	Impact (Gross)
1	Breach of contractual clauses, modification of agreed terms, rates, deadlines, guarantees without the consent of involved parties.	2-Medium	3-High	High
2	System failures related to equipment, software, applications, or communication infrastructure.	1-Low	1-Low	Low
3	Parameter configuration failure in Databricks.	3-Medium	2-Medium	Medium
4	Failure in procedures and/or application of internal/external standards (Lack of control tools to monitor the execution of required internal and external norms by regulatory bodies).	3-High	3-High	High

The Impact result (Gross) is obtained according to the positioning of the Probability and Severity values of each risk in the Probability x Severity Matrix graph (Table 2).

The distribution of the Probability and Severity coordinates of each risk in a region of the matrix shown in the Table 3 - Risk classified in the region, defines the classification of the risk level, as follows.

Table 3 - Risk classified

Graph region	Impact	Risk appetite
Green	Low	**Inside**
Yellow	Medium	
Orange	Very high	**Outside**
Red	Very high	

Therefore, for the processing of personal data of the services subject to analysis of this RIPD, the classification of the level of risks identified was distributed as follows in Table 4 – Risk Matrix (Inherent).

Table 4 – Risk Matrix (Inherent)

Assessment Risks Step:		**Inherent**	**Residual**	**Planned**
		X	--	--
Very High	#Risks			#Risks
High			#Risks	
Medium				
Low	#Risks	#Risks		
4x4	**Low**	**Medium**	**High**	**Very High**

At this stage, the matrix must contain the risks inherent at the beginning of the process (gross risk), without the application of controls.

3. Need for the Report

Justify why the RIPD is necessary. Highlight specific data processing activities that involve sensitive or personal data and explain how these activities might impact the rights and freedoms of data subjects.

- **LGPD Reference**: Art. 7º, IV.
- **Compliance**: Justifies the need for data processing based on legal grounds, ensuring that processing is lawful and necessary.
- **Example Scenario:** The company processes employee data like names and payroll details for HR management and legal compliance.

4. Description of Data Processing

Outline the nature, scope, context, and purpose of data processing. Include details such as the type of data collected, how it is processed, and the technological tools used.

i. **Nature of Processing**: Describe the type of data being processed (e.g., personal data, sensitive data).

ii. **Scope of Processing**: Detail the extent and boundaries of data processing activities.

iii. **Context of Processing**: Provide context on why the data is being processed, considering business or operational needs.

iv. **Purpose of Processing**: Clearly define the intended outcomes or goals of the data processing.

- **LGPD Reference**: Art. 6º, III (necessity).
- **Compliance**: Ensures data processing is limited to what is necessary, directly addressing the principle of data minimization.
- **Example Scenario:** The Industries collects only essential employee data, such as IDs and bank details, strictly for payroll and tax compliance purposes.

5. Stakeholders Consulted

Identify the individuals or groups consulted during the preparation of the RIPD. This might include internal stakeholders like IT security experts, legal consultants, compliance officers, and business unit representatives, as well as external consultants.

- **LGPD Reference**: Art. 41.
- **Compliance**: Involves consulting stakeholders, including the DPO, aligning with the requirements for ongoing oversight and data protection management.
- **Example Scenario:** The company identifies risks, such as unauthorized access, and mitigates them through access controls and regular audits.

6. Necessity and Proportionality

Provide the legal basis for data processing, emphasizing data minimization principles and compliance with data protection laws.

i. **Legal Basis**: Explain the legal grounds for data processing, such as consent, legitimate interest, or contractual necessity.

ii. **Data Minimization**: Highlight efforts to collect only the minimum necessary data to achieve the intended purposes.

- **LGPD Reference**: Art. 6º, III and IV.
- **Compliance**: Evaluates and ensures data processing is proportional to its intended purpose, preventing excessive data handling.
- **Example Scenario:** The Industries consults its Legal and IT departments and an external cybersecurity firm to evaluate data protection measures.

7. Risk Identification and Assessment

Describe the technical and organizational measures implemented to address identified risks, including data encryption, access controls, and monitoring protocols.

- **Risk Identification**: List the potential risks to data subjects, such as unauthorized access, data breaches, or loss of data integrity.
- **Risk Assessment**: Assess the likelihood and severity of each risk, categorizing them as low, medium, or high impact.

- **LGPD Reference**: Art. 6º, VII (security).
- **Compliance**: Identifies and evaluates risks, ensuring data processing is secure and risks are mitigated as required by LGPD.
- **Example Scenario:** The company implements two-factor authentication, data encryption, and regular employee training on data protection.

8. Mitigation Measures

Describe the technical and organizational measures implemented to address identified risks, including data encryption, access controls, and monitoring protocols.

i. **Technical Measures**: Detail the technical safeguards, such as encryption, pseudonymization, access controls, and regular security audits.

ii. **Organizational Measures**: Include policies, staff training, and procedures designed to ensure compliance with data protection laws.

- **LGPD Reference**: Art. 46.
- **Compliance**: Implements measures to protect personal data against unauthorized access, ensuring security controls are in place.

Data processing agents must adopt security measures, both technical and administrative, to protect personal data from unauthorized access and accidental or illegal situations of destruction, loss, alteration, communication, or any other form of improper or unlawful processing (LGPD, Art. 46).

In the "Controls" column of the table Table 5 – Exemple of proposed controls for each risks the security measures or specific controls adopted for managing the risks identified of this Report are defined.

The institution does not always need to address all risks. In this sense, it can be decided that some risks are acceptable (risk appetite) — up to a medium risk level — due to the benefits of processing personal data and the difficulties in mitigation. However, if, after implementing the proposed controls, a high or very high risk level remains, it is advisable to consult the ANPD (National Data Protection Authority of Brazil) before proceeding with personal data processing operations.

Table 5 – Exemple of proposed controls for each risks

Code [1]	Risk	Controls [2]	Effect on Risk [1]	Impact (Residual) [3]
1	Unauthorized access to sensitive data due to weak password policies.	1- Implementation of multi-factor authentication, 2- Regular password strength checks and user training.	Reduce	Low
2	Failure of backup systems leading to potential data loss.	3- Regular testing of backup systems, 4- Implementing redundant backup locations.	Reduce	Low
3	Incorrect configuration of cloud access permissions.	5- Role-based access control, 6- Regular audit of permissions, 7- Training for cloud administrators.	Reduce	Medium
4	Lack of encryption for data in transit across internal networks.	8- Implement encryption protocols for internal data transit, 9- Regular network security assessments.	Reduce	Low
5	Unmonitored use of third-party APIs in critical business applications.	10- Continuous monitoring of API usage, 11- Secure API gateways, 12- Regular review of third-party access logs.	Reduce	Low
6	Failure to update security patches on critical systems in a timely manner.	13- Automated patch management system, 14- Weekly review of critical system updates and patch status.	Reduce	Low

[1] Effect resulting from the treatment of the risk with the application of the measure(s) described in the table. The following options can be selected: **Reduce, Avoid, Share and Accept.**

[2] Measure approved by the controller of the personal data.

[3] Residual impact after the proposed controls have been applied.

Table 6 – Risk Matrix (Planned)

Assessment Risks Step:		Inherent	Residual	Planned
		--	--	X
Very High	#Risks			#Risks
High			#Risks	
Medium				
Low	#Risks	#Risks		
4x4	**Low**	**Medium**	**High**	**Very High**

9. Approval

Document the approval process, including signatures from the responsible authorities. Mention that the RIPD should be reviewed and updated regularly or whenever significant changes occur in data processing activities.

- **LGPD Reference**: Art. 50 (best practices).
- **Compliance**: Formalizes the approval process, ensuring continuous monitoring and updating of data protection measures.
- **Example Scenario:** The RIPD is reviewed and approved by the Compliance Officer, with scheduled reviews every six months to ensure ongoing compliance.

This section aims to formalize the approval of the RIPD through obtaining signatures from the individual responsible for preparing the RIPD, the Data Protection Officer, and the authorities representing the controller and operator. The person responsible for preparing the Report can be the Data Protection Officer or any other person designated by the controller with the necessary knowledge to perform this task.

The RIPD must be reviewed and updated annually or whenever there is any change that affects the processing of personal data carried out by the institution. Details on the need for

reviewing the RIPD can be found in item 2.5.2.9 of the LGPD Good Practice Guide, available at:

https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf.

RESPONSIBLE FOR THE PREPARATION OF THE IMPACT REPORT

DATA PROTECTION OFFICER

<Name of the Responsible Person>

<Department / Area> Local, <day> of <month> of <year>

RESPONSIBLE FOR INFORMATION SECURITY

<Name of the Representative>

<Department / Area> São Paulo, <day> of <month> of <year>

RESPONSIBLE FOR LEGAL ASPECTS

<Name of the Representative>

<Department / Area> São Paulo, <day> of <month> of <year>

10. Final Considerations

This explanation guides the inclusion of detailed, relevant information in each section, ensuring the RIPD is comprehensive and tailored to meet the legal and operational requirements of data protection.