IDENTIFICATION AND ASSESSMENT OF ELIGIBILITY CRITERIA FOR PREPARING THE PERSONAL DATA PROTECTION IMPACT ASSESSMENT (RIPD)

Rainier Garacis [*]

Abstract: This study aims to analyze the criteria that determine whether personal data processing requires the preparation of a Data Protection Impact Assessment (RIPD) and its relevance for compliance with the Brazilian General Data Protection Law (LGPD). The RIPD is an essential tool for assessing risks in personal data processing, enabling organizations to identify, measure, and mitigate potential impacts on privacy and security. With the exponential growth of data collection, storage, and processing in digital environments, understanding the legal and methodological requirements involved in its preparation is crucial. The research addresses the key quantitative and qualitative factors that determine the necessity of conducting a RIPD, as well as the practical challenges organizations face in identifying these elements. Additionally, the role of regulatory authorities, such as the Brazilian National Data Protection Authority (ANPD), in overseeing and requiring this document for certain data processing activities is discussed. The study also compares the eligibility criteria for the RIPD with international guidelines, such as those established by the European Union's General Data Protection Regulation (GDPR), aiming to understand similarities, differences, and potential challenges in adapting to the Brazilian context. Finally, the challenges and benefits of implementing the RIPD are analyzed, highlighting its importance in fostering a data protection culture and ensuring greater legal security for companies and institutions engaged in personal data processing.

Keywords: General Data Protection Law (LGPD); Data Protection Impact Assessment (RIPD); High Risk.

INTRODUCTION

The personal Data Protection Impact Assessment (RIPD) is an essential tool in the context of the General Data Protection Law (LGPD). Established by Article 5 of the LGPD, the RIPD is defined as a detailed documentation of data processing that may generate risks to civil liberties and fundamental rights of individuals. This report not only describes these processes, but also proposes measures, safeguards, and risk mitigation mechanisms appropriate to the specific case. The importance of the RIPD is reflected in its mandatory nature for personal data controllers, standing out as an important component

[*] Post-graduate in Digital Law from the Institute for Technology and Society of Rio de Janeiro, Brazil. Email: r.garacis@hotmail.com / ORCID iD: https://orcid.org/0009-0003-9847-7842

in the governance of personal data and in the management of risks associated with its processing, reinforcing the trust of data subjects regarding the management of their personal information[1].

Despite the conceptual clarity offered by the LGPD, the practical implementation of the RIPD presents several challenges. Among them, the correct and coherent identification of the eligibility criteria for the preparation of the report stands out. These criteria are crucial to ensure that the processing of personal data that involves high risk is properly documented and has its risks identified and mitigated appropriately. The National Data Protection Authority (ANPD) plays a fundamental role in defining these criteria, as described in article 55-J of the LGPD. However, subjectivity and the lack of detailed regulation have generated uncertainty among data controllers about when and how to prepare the RIPD[2].

Furthermore, the implementation of the RIPD requires constant adaptation by data controllers, especially in a new and unregulated scenario. Therefore, the role of the ANPD in pursuing the definition of clear parameters on when and how the RIPD should be prepared is crucial to minimize the uncertainties that still exist in the current scenario. In addition, training companies and promoting an organizational culture that values the protection of personal data are essential to ensure that RIPDs are not seen merely as a legal requirement but as a strategic governance and risk management tool. The European approach, in turn, serves as a parameter for the topic in Brazil, highlighting the need for a maturation of national regulations so that data controllers can fulfill their obligations more clearly and efficiently, ensuring the protection of the rights of data subjects.

Furthermore, this article explores the practical challenges faced by data controllers in identifying eligibility criteria for the RIPD, drawing on current guidance, such as Resolution No. 2 and the public consultation on the Guidance on High-Risk Processing, both documents created by the ANPD. Furthermore, it compares the Brazilian approach with the European one, highlighting similarities and differences in regulation and practice. By addressing these issues, the article seeks to provide a comprehensive overview of the complexities involved in implementing the RIPD and possible solutions to overcome the practical challenges that arise in the context of personal data protection.

---

[1] Gomes, Maria Cecília O. 2019. "Beyond a 'Legal Obligation': What the Benefits and Risks Methodology Teaches Us about the Data Protection Impact Report." In *Digital Law: Contemporary Debates*, edited by Ana Paula Lima, Carmina Hissa, and Paloma Mendes Saldanha, 141–153. São Paulo: Revista dos Tribunais.

[2] Gomes, Maria Cecília. 2021. "Data Protection Impact Report: Mandatory for the Processing of Sensitive Data?" In *LGPD in Health*, edited by Analluza Bolivar Dallari and Gustavo Ferraz Monaco, 263–275. São Paulo: Thomson Reuters Brazil.

I. WHAT IS A PERSONAL DATA PROTECTION IMPACT ASSESSMENT (RIPD)?

The concept of a personal Data Protection Impact Assessment was established in the LGPD itself through art. 5, defining it as a documentation of the personal data controller that contains the description of the personal data processing that may generate risks to civil liberties and fundamental rights, as well as measures, safeguards, and risk mitigation mechanisms[3]. Although the concept is relatively simple, the RIPD, on the other hand, currently presents numerous complexities, such as the necessary elements that must be included, eligibility criteria, publicity of the report, time of preparation, etc. [4].

Furthermore, the LGPD, in its art. 38, defines that one of the mandatory risk governance measures that personal data controllers must adopt is the creation of a personal Data Protection Impact Assessment (RIPD):

> Art. 38. The national authority may order the controller to prepare a report on the impact on the protection of personal data, including sensitive data, regarding its data processing operations, in accordance with the regulation, taking into account commercial and industrial secrets.
>
> Sole paragraph. In compliance with the provisions of the caput of this article, the report must contain, at a minimum, a description of the types of data collected, the methodology used for collection and to ensure the security of the information, and the controller's analysis of the measures, safeguards, and risk mitigation mechanisms adopted.

This report must be composed of (I) a description of the personal data processing that may generate risks to the civil liberties and fundamental rights of the data subjects involved in the respective processing, as well as (II) measures, safeguards, and mechanisms to mitigate the risks identified throughout the preparation of this report. Through it, it is possible to demonstrate what risks exist for the subjects within the context of the process analyzed and what safeguards were implemented by the controller to mitigate them, preferably, before carrying out the processing involving personal data, as provided by the National Data Protection Authority (ANPD) itself,

---

[3] Gomes, Maria Cecília. 2021. "Data Protection Impact Report: Mandatory for the Processing of Sensitive Data?" In *LGPD in Health*, edited by Analluza Bolivar Dallari and Gustavo Ferraz Monaco, 263–275. São Paulo: Thomson Reuters Brazil.

[4] Brazil. 2018. *Lei No. 13.709, de 14 de Agosto de 2018 (Lei Geral de Proteção de Dados).* Accessed June 21, 2025. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

precisely so that it is possible to assess, in advance, the possible risks associated with this processing (Privacy by Design)[5].

In this way, the controller will be able, even before using personal data for that purpose, to identify the probability of occurrence of each risk factor and its impact on the fundamental freedoms and rights of the data subjects and adopt the measures, safeguards and risk mitigation mechanisms appropriate to the hypothesis or, as a last resort, not proceed with the processing[6].

It is important to emphasize that the risk associated with the impact report must consider the rights and freedoms of the holder of personal data as the fundamental prism of the analysis and not the business or compliance risk in relation to decision-making on data processing. As Maria Cecília Oliveira Gomes explains:

> "(...) this type of (business) risk, wrongly associated with the report, is a risk much more focused on an aspect of regulatory compliance "*compliance risk* ", than on a risk associated with rights. In this sense, it is worth reinforcing this difference, since apparently many have confused the risk in the adequacy process with the risk indicated in the impact report."[7]

II. TREATMENT ELIGIBILITY CRITERIA REQUIRING RIPD

Given the importance of the existence of the RIPD mentioned above, it is necessary for controllers to correctly and coherently identify which treatments are appropriate for reporting. Since, although its existence does not guarantee full compliance or total mitigation of the risks inherent to the treatments, it is one of the main mechanisms of the LGPD to ensure an acceptable level of risk in the processing of personal data, becoming a fundamental element to demonstrate the compliance, good faith, and concern of controllers with the data of the data subjects processed.

To identify these criteria, it is necessary to observe, primarily, art. 55-J of the LGPD, which sets out one of the ANPD's powers, consisting of issuing regulations and guides about the RIPD, including, but not limited to, the

---

[5] Lohmann, Pedro A., and Raphael Carlos Albuquerque. 2021. "Systematic Review for the Data Protection and Privacy Impact Assessment Process." Unpublished manuscript.

[6] ANPD (Autoridade Nacional de Proteção de Dados). 2023b. *Resolution CD/ANPD No. 11, of December 27, 2023.* Gov.br. Accessed June 21, 2025. https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-11-de-27-de-dezembro-de-2023-534947737.

[7] Gomes, Maria Cecília. 2021. "Data Protection Impact Report: Mandatory for the Processing of Sensitive Data?" In *LGPD in Health*, edited by Analluza Bolivar Dallari and Gustavo Ferraz Monaco, 263–275. São Paulo: Thomson Reuters Brazil.

necessary criteria to be observed by personal data controllers to create the report.

> Art. 55-J. The ANPD is responsible for: (...)
>
> XIII - to issue regulations and procedures on the protection of personal data and privacy, as well as on reports on the impact on the protection of personal data for cases in which the processing represents a high risk to the guarantee of the general principles of protection of personal data provided for in this Law.

This section shows the presence of the key element that will be used to identify the eligibility criteria: the high risk to the guarantee of the general principles of personal data protection. It is through this concept that the ANPD seeks to propose which criteria are considered central to those treatments considered to be high risk. These criteria will be presented and addressed throughout this article[8].

In addition to the premise presented in art. 55-J of the LGPD, the legal text also presents two other possible criteria that may give rise to the need to proceed with the procedure for preparing the RIPD. Although little explored in the LGPD and pending active action by the national authority itself, these are the cases of arts. 10, §3, and art. 38 of the LGPD, which indicate that the ANPD may (not being a rule) request controllers to prepare the RIPD for, respectively, some cases in which the processing has as a legal hypothesis the legitimate interest and processing that uses sensitive personal data[9].

Although the texts of the provisions are clear and direct, that is, if the legal basis is legitimate interest or sensitive personal data is processed, a RIPD must be drawn up, the legislator chose not to treat these criteria as absolute or objective and did not even treat them as mandatory criteria, which may be a necessity depending on the regulator's request to the controller[10]. It is necessary to wait for specific regulation on the subject from the national authority, as reinforced by Maria Cecília Oliveira Gomes:

> "The LGPD did not expressly provide for the situations in which the impact report would be mandatory. What the LGPD indicates is the situations in which the ANPD, within its powers, can or should

[8] Lohmann, Pedro A., and Raphael Carlos Albuquerque. 2021. "Systematic Review for the Data Protection and Privacy Impact Assessment Process." Unpublished manuscript.

[9]Sensitive personal data is, based on art. 5, II of the LGPD, personal data about racial or ethnic origin, religious belief, political opinion, membership of a union or organization of a religious, philosophical or political nature, data relating to health or sexual life, genetic or biometric data, when linked to a natural person;

[10] Dozza, Eleonora Coelho. 2023. "Secondary Use of Personal Data and Its Basis in Legitimate Interest in Post-LGPD Brazil." Accessed June 21, 2025. https://lume.ufrgs.br/bitstream/handle/10183/264345/001173367.pdf.

> request the impact report from a controller in a broad manner or in specific processing contexts. Likewise, the LGPD did not indicate what a high-risk processing operation is, it only indicated that it is the ANPD's responsibility to develop guidelines on the subject."[11]

As a consequence of this objective lack of definition brought by the legislator, Matheus Sturari highlights, by way of example, the numerous uncertainties presented by treatment agents in practice:

> It can be seen, by deduction from the definition in art. 5, XVII, that the DPIA[12] will be required for processing activities that generate risks to civil liberties and fundamental rights. However, several doubts remain, for example: (i) must every hypothesis of processing based on legitimate interest be accompanied by a DPIA?; (ii) which processing operations will be considered as generating risks to the point of requiring a DPIA?; (iii) despite a list, which criteria should be considered to analyze the existence of risk and consider the need for a DPIA?; (iv) must each and every risk give rise to a DPIA or only a "high" risk, as in item XIII of art. 55-J? (...) It turns out that the existence of such doubts and a scenario of uncertainty surrounding the topic has generated an effect that, in my view, may not be positive: the possible trivialization of the DPIA and consequent excessive burden on processing agents."[13]

In this sense, Felipe Fontes Cabral agrees with this lack of objective criteria: "(...) there is a risk that the RIPD will become a control instrument in isolated cases or, worse, that it will be a document prepared for formal purposes, but without guiding a real risk management activity, which may compromise the effectiveness of the personal data protection system in Brazil."[14]

It is also important to mention that the ANPD, when establishing the criteria in future regulations, must exercise caution and ensure proportionality between the formal need for the RIPD and the real purpose of the report.

---

[11] Gomes, Maria Cecília. 2021. "Data Protection Impact Report: Mandatory for the Processing of Sensitive Data?" In *LGPD in Health*, edited by Analluza Bolivar Dallari and Gustavo Ferraz Monaco, 263–275. São Paulo: Thomson Reuters Brazil.

[12] DPIA is the acronym translated into English for RIPD.

[13] Sturari, Matheus. 2020. "The DPIA in the LGPD: National Interpretation or Trivialization of the Instrument?" LinkedIn, July 22, 2020. Accessed June 21, 2025. https://www.linkedin.com/pulse/o-dpia-na-lgpd-interpretação-nacional-oubanalização-do-matheus/.

[14] Cabral, Filipe Fonteles. 2019. "The Personal Data Protection Impact Report as an Instrument for Risk Management in the General Personal Data Protection Law." In *Special Notebook: General Data Protection Law (PGPD)*, 200–211. São Paulo: Revista dos Tribunais.

Since, if it "gets it wrong", it may excessively burden controllers and operators with a possible merely formal legal obligation, without any practical importance for controlling privacy risks, which goes against the preventive system brought by the LGPD[15].

A. Resolution No. 2/ANPD and High-Risk Guide

Based on the premises reported in the previous chapter, the ANPD has not yet chosen the criteria for preparing the RIPD. However, through a public consultation with society regarding the new Guidance Guide for High-Risk Treatments for, but not limited to, Small-Scale Treatment Agents (ATPP), it presented a proposal for which criteria may be considered relevant for this identification.

Although ANPD Resolution No. 2 of 2022 does not, at first glance, have a direct correlation with the RIPD theme, since it deals with the definition and parameters of Small-Scale Treatment Agents (ATPP), it is through this device that the regulator decided to present what would be considered high-risk treatments and what the methodology for evaluating eligibility criteria is.

The methodology in question indicates that the personal data controller must assess the existence, in the processing of personal data, of at least one general criterion combined with a specific criterion, as established in art. 4 of the aforementioned Resolution.

> Art. 4 For the purposes of this regulation, (...) the processing of personal data that cumulatively meets at least one general criterion and one specific criterion, among those indicated below, will be considered high risk:
> I - general criteria:
> a) processing of personal data on a large scale; or
> b) processing of personal data that may significantly affect the interests and fundamental rights of the data subjects;
> II - specific criteria:
> a) use of emerging or innovative technologies;
> b) surveillance or control of areas accessible to the public;
> c) decisions taken solely on the basis of automated processing of personal data, including those intended to define the personal, professional, health, consumer and credit profile or aspects of the data subject's personality; or

[15] Grasso, Ian Matiello. 2021. "Impact Report on the Protection of Personal Data in the General Data Protection Law: A Trivialization?" *Legal Notebooks of the Sorocaba Law School – Digital Law* 3 (1): 142–174.

> d) use of sensitive personal data or personal data of children, adolescents and the elderly[16]. (ANPD, 2022)

Therefore, even though the high-risk calculation methodology was created to comply with a resolution that is not directly related to the central topic addressed in this article, it is through the public consultation of the Guidance for High-Risk Treatments that the ANPD confirms the recommendation to use these criteria and methodology to select which treatments should have RIPD until there is a specific resolution on the topic[17]. In fact, before the public consultation of the guide, the ANPD, through the FAQ on RIPD, had already recommended that controllers use the same criteria set out to identify high-risk treatments in ANPD Resolution No. 2 of 2022[18]. However, until that moment, there was no clarity on how to practically evaluate the elements of the criteria set out in art. 4 of this resolution, and there was not even any documentation created by the Regulatory Agency that formalized this recommendation.

Even though the high-risk guide is the document prepared by the ANPD that is closest to what would be recommended to be taken into consideration, it should be remembered that the regulator itself indicates that these criteria and methodology will not replace new specific regulations on the subject or even exhaust their applicability in practical cases. It is up to the controllers to identify the need to sequence the RIPD even if the processing does not have the presence of the aforementioned criteria[19].

---

[16] ANPD (Autoridade Nacional de Proteção de Dados). 2022. *Resolution CD/ANPD No. 2, of January 27, 2022.* Gov.br. Accessed June 21, 2025. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022.

[17] Item 5 of ANPD Resolution No. 11 of 2023 indicates that the RIPD issue is being addressed by the authority with new regulations expected for the 2023-2024 biennium. The topic has not been exhausted with the high-risk and large-scale guide.

[18] ANPD (Autoridade Nacional de Proteção de Dados). 2022. *Resolution CD/ANPD No. 2, of January 27, 2022.* Gov.br. Accessed June 21, 2025. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022.

[19] "It should be noted that, for the purposes of preparing the RIPD, these criteria should not be considered exhaustive, so that the controller may verify the existence of high risk in situations other than those indicated. Thus, in accordance with the principle of accountability and accountability, it is up to the controller to assess the relevant circumstances of the specific case, in order to identify the risks involved and the appropriate prevention and security measures, considering the possible impacts on the fundamental freedoms and rights of the data subjects and the likelihood of their occurrence" (ANPD (Autoridade Nacional de Proteção de Dados). 2023a. *Personal Data Protection Impact Report (RIPD).* Gov.br. Accessed June 21, 2025. https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd).

1. Entering the High-Risk Criteria

In view of the above, the guide in question has the main objective of providing greater details on how to identify, for example, whether a given treatment meets the general eligibility criteria of the RIPD, that is, whether it has large-scale elements or significantly affects the rights and freedoms of the data subjects.

Regarding these criteria, it is worth mentioning that the large-scale analysis will only observe quantitative elements of the processing, while the criteria that makes it possible to assess the significant impacts on the data subjects will only observe qualitative elements, referring to the magnitude of the impacts that the personal data processing activity may have on the interests and fundamental rights of the data subjects. Therefore, a detailed and well-founded assessment of its possible negative consequences is required, that is, the possible impacts that may be generated by the processing of the subjects' data[20].

The ANPD also established that, to assess the large-scale criterion, it is necessary to apply a mathematical formula that will consider the following elements: number of data subjects affected by the processing, average volume of data processed (to identify the average volume of data processed, the controller must divide the number of data subjects involved in the processing by the total number of data records processed), frequency (number of times the processing is carried out over time), duration (length of time the processing lasts until the personal data is deleted) and geographic extent (identification of the scope and reach of the processing operation). This mathematical formula attaches different weights to each of these elements, affecting the final result depending on the specific case. It is important to mention that the number of data subjects affected is the main element of the formula, having considerably greater weight in identifying the large scale in relation to the others[21].

The formula, in itself, does not present great complexity of development: based on the identification of the elements of the practical case, each of them will have specific weights (presented through the table of values present in the guide) that will be added at the end of the controller's analysis and, if the sum of the weights results in a value greater than twenty-five (25),

[20] ANPD (Autoridade Nacional de Proteção de Dados). 2024. *Public Consultation – Guidance on the Processing of High-Risk Personal Data.* Gov.br. Accessed June 21, 2025. https://www.gov.br/participamaisbrasil/blob/baixar/48651.

[21] ANPD (Autoridade Nacional de Proteção de Dados). 2024. *Public Consultation – Guidance on the Processing of High-Risk Personal Data.* Gov.br. Accessed June 21, 2025. https://www.gov.br/participamaisbrasil/blob/baixar/48651.

the evaluated treatment must be classified as large scale[22].

Regarding the general qualitative criterion of high risk: significantly affecting fundamental rights and freedoms, it must be assessed subjectively by the controller based on the following elements: possibility of the processing operation causing moral or material damage, preventing the exercise of fundamental rights or preventing the use of essential services.

The key concept that should be used to assess the criteria indicated above is the identification of the severity and likelihood of an illegitimate and unreasonable impact on the interests and rights of the data subjects involved in the processing. Any impacts that are limited, proportionate or necessary for the fulfillment of legitimate purposes or for the exercise of rights should not be taken into account when classifying the processing under this criterion. In addition, in relation to those processing operations that may cause moral or material damage, the ANPD presents some practical examples of what may be considered to assess the existence of this element in the processing in question, namely: possibility of causing discrimination, violation of physical integrity, the right to image and reputation, financial fraud or identity theft[23].

Regarding specific criteria, although they are significantly more objective than the analysis of the general criteria presented previously, there is still a certain degree of subjectivity that must be addressed by controllers in a justified manner, as is the case with the criterion of emerging or innovative technologies, for example.

B. Comparison of the criteria recommended in Brazil and those established in Europe

The basis built in the LGPD was inspired by European legislation, with some adaptations for the Brazilian scenario. This inspiration brought several obligations and instruments also present in the GDPR (European regulation on the protection of personal data). This is the case of the RIPD being equivalent to the European Data Protection Impact Assessment (DPIA)[24].

The Data Protection Impact Assessment (RIPD), although a recent

---

[22] The ANPD has established that cases of personal data processing involving more than two million data subjects are already considered high risk, that is, they will already reach the objective value of high risk (twenty-five). It is necessary to assess the other large-scale elements (frequency, duration, geographic extension and average volume of data) only in cases where the volume of data subjects involved in the processing is less than two million.

[23] ANPD (Autoridade Nacional de Proteção de Dados). 2024. *Public Consultation – Guidance on the Processing of High-Risk Personal Data.* Gov.br. Accessed June 21, 2025. https://www.gov.br/participamaisbrasil/blob/baixar/48651.

[24] Grasso, Ian Matiello. 2021. "Impact Report on the Protection of Personal Data in the General Data Protection Law: A Trivialization?" *Legal Notebooks of the Sorocaba Law School – Digital Law* 3 (1): 142–174.

topic in Brazil, already has a more robust and mature scenario in Europe. Thus, in this subchapter, the main objective will be to explore some of the criteria established in Europe compared to those we currently have in Brazil, bringing the European perspective of the processing "likely to entail a high risk to the rights and freedoms of the data subject".

In the European scenario, as in Brazil, local legislation has not detailed the criteria for data processing agents to have a clear idea of which processing operations could generate a high risk to data subjects and, consequently, should carry out a Data Protection Impact Report. This is why, even before the publication of the GDPR, the now-defunct Article 29 Working Party[25] prepared one of the oldest and most relevant *guidelines* on the subject. This is the document "Guidance on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation (EU) 2016/679", prepared in 2017 and endorsed by the current European Data Protection Board[26].

Unlike Brazil, which has only one regulator (ANPD), the European scenario is made up of numerous countries and, obviously, different regulators among them. Thus, the *guideline* in question presents a broad and common rationale so that the member countries of the European bloc have, at the very least, similar and basic criteria for assessing high risk, which can be detailed according to the understanding of the numerous existing Regulators and the realities of the countries.

When comparing both guides prepared for high risk, we can identify numerous correlations between the criteria and rationales adopted for analyzing treatments. The first that can be identified is the indication that, although the criteria of both guides are a broad guide for analyzing treatment agents, they are only examples and are not exhaustive. In other words, there may be other treatments, including those that do not meet any of the eligibility criteria, and even so, it will be necessary for the controllers to prepare the report. There is a need for the controllers to evaluate each specific case carefully and, if the relevance of preparing the report is identified, to execute it.

Other aspects of similarity are in relation to the eligibility criteria themselves, although the evaluation methodology is different.

When observing the European criteria, it can be identified that six (6) of

---

[25] Article 29 Data Protection Working Party. 2017. *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation (EU) 2016/679.* Accessed June 21, 2025. https://ec.europa.eu/newsroom/article29/items/611236.

[26] European Data Protection Board. 2018. "Endorsement of the Working Party 29 Guidelines on GDPR by the EDPB." Accessed June 21, 2025. https://www.edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.

the nine (9) criteria present in the *guideline* have relevant synergy with those recommended by the ANPD, including the rationale that should be taken into consideration for their evaluation, which are: preventing data subjects from exercising a right or using a service or contract, use of innovative solutions or application of new technological or organizational solutions, data relating to vulnerable data subjects, data processed on a large scale (with the exception of the absence of analysis of the frequency element, all others are present in the identification of the large-scale criterion), sensitive data and systematic control, but not only of areas accessible to the public.

Regarding the criteria that do not have a direct correlation, they are: evaluation or classification (profiling and prediction of data subjects), automated decisions that produce legal effects or significantly affect data subjects in a similar way (although the criterion of significantly affecting data subjects is a premise present in the national criteria, the European scenario limits this premise to those decisions that are taken automatically) and establishing a set or combination of data collected for purposes other than those intended to carry out the processing operation[27].

Regarding the evaluation methodology, in the European scenario there is no subdivision of general and specific criteria, they all have the same weight and must be evaluated separately, with the DPIA being carried out if the same treatment has more than two eligibility criteria, whatever they may be. The greater the number of criteria present in the treatment, the greater the likelihood of it being necessary to carry out the RIPD.

In Brazil, according to the high-risk guide, the processing may, in theory, according to the analysis methodology, have all the specific criteria present and still not be required to carry out the RIPD. Given that the general criteria are the main elements for electing a processing as high risk (large scale or high probability and severity of significantly affecting the rights and freedoms of the holders).

III. PRACTICAL CHALLENGES IN IDENTIFYING THE CRITERIA RECOMMENDED BY THE ANPD

Identifying eligibility criteria in Brazil presents significant challenges due to the lack of detailed regulation and the subjective nature of some of the criteria established by the LGPD, as presented throughout this article.

Therefore, one of the difficulties that controllers may face in practice is in relation to the large-scale criteria. Although the formula offers an objective

[27] Article 29 Data Protection Working Party. 2017. *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation (EU) 2016/679.* Accessed June 21, 2025. https://ec.europa.eu/newsroom/article29/items/611236.

structure, the application of quantitative elements and the assignment of weights may generate doubts and difficulties, especially in contexts that do not fit perfectly within the established parameters. This difficulty is related to the maturity of the controller in relation to the clarity and detail of the mapping of its processes and databases, including the lack of tools capable of mapping unstructured data. In this scenario, simple activities, such as customer service, may present complexities in accurately gathering the information necessary to assess this criterion. Questions such as: "How much personal data is processed, including by email?" or "What is the geographic extension of the data subjects (increasing the complexity if location information is not collected when serving data subjects)?" may be raised by these processing agents if they do not have mature processes and/or personal data mapping tools[28] that will assist in the precise identification of structured and, mainly, unstructured data[29].

Still regarding the general criteria, assessing whether the processing may significantly affect the holders of personal data is, in itself, a procedure that raises numerous doubts about the rationale that controllers should develop to reach a conclusion. In fact, the High Risk Guidance Guide, to date, does not present, demonstrate or develop a clear rationale to guide the analyses of the elements that define this criterion; it merely presents a few examples. Therefore, one of the possible controls to demonstrate the good faith and responsibility of controllers is to develop governance procedures so that qualitative analyses of the processing are recorded and form part of the record of personal data processing, making it possible to present, in a substantiated manner, the argumentative points that concluded the existence or not of this criterion.

---

[28] "The process of mapping personal data is essential to support the process of managing privacy and information security risks. It involves identifying customer, supplier and employee data. Mapping aims to provide the initial information so that the organization can achieve and maintain compliance with the law.

This process aims to identify which data is in possession (...) and ensure its privacy, safeguarding the institution if it should face problems with leaks, complaints and the like." (LCNN (National Laboratory for Scientific Computing). 2024. "What Is Personal Data Mapping?" Gov.br. Accessed June 21, 2025. https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/gestao-de-seguranca-da-informacao/o-que-e-mapeamento-de-dados-pessoais)

[29] Structured data is data that is represented by numbers, tables, rows, columns, attributes, and so on. As the name implies, structured data is generally disciplined, well-behaved, predictable, and repeatable. Unstructured textual data is simply a collection of characters, such as data found in emails, reports, documents, medical records, and spreadsheets. This type of data has no format, no structure, and no repetition. (Barbosa, Elaine Muniz. 2016. "Integration of Social Network Data into Data Warehouses." Master's thesis, Federal University of Minas Gerais. Accessed June 21, 2025. http://hdl.handle.net/1843/ESBF-AKUNG3)

It is worth mentioning that the criteria for defining the use of emerging or innovative technologies have the same theoretical difficulty as the assessment of significant impacts. There is no centralized list, for example, by the ANPD defining a range of technologies in this sphere. It is up to the controllers to carry out this type of analysis based on their own assessments and market convictions, which can generate insecurity for the national ecosystem of personal data protection.

Another point that could be questioned is the innovation presented by the ANPD that sought to equate the elderly with children and adolescents. Analyzing this criterion based on the guide prepared, the mere availability for sale of products or services in the market, in turn, may already qualify this criterion as existing in the processing, since in order to carry out the procedures for selling and sending the product or providing the service, it is necessary to process personal data and, as a rule, there is no type of control that obviously prevents the elderly from consuming any products and services widely displayed in the market.

As this criterion is established today, any large company that sells products or services to more than two million customers will probably need to carry out a RIPD for those treatments involved in the execution of purchase and sale contracts, regardless of the notion of privacy risks linked to them, distorting the very objective of the guide and the definition of high risk.

With the examples addressed above, it is clear that the lack of clear guidelines on when exactly RIPD becomes mandatory adds a certain level of uncertainty for data controllers, who must determine whether reporting is necessary based on their own interpretation of the circumstances.

The difficulty is further exacerbated by the absence of specific regulations addressing RIPD, leading controllers to rely on general guidelines and best practices established by other regulations and guidelines. The ANPD's recommendation to use the criteria of Resolution No. 2 as a reference, although useful, does not replace the need for dedicated and specific regulations for RIPD, which could provide greater clarity and legal certainty to the national scenario of privacy and personal data protection.

CONCLUSION

The preparation of a RIPD is an essential practice to ensure compliance with the LGPD and the protection of data subjects' rights. However, identifying the eligibility criteria for the RIPD presents significant challenges, mainly due to the lack of specific regulation and the subjectivity of some criteria established by the ANPD. The recommended methodology, which is based on the composition of general and specific criteria, provides a basis, but also requires controllers to make an effort to carry out a careful

and well-founded analysis of their data processing, which can cause practical difficulties for controllers who do not have maturity on the subject.

The lack of clear and detailed guidelines increases the complexity of criteria assessments and can generate uncertainty for data controllers. However, adopting robust data governance practices, including detailed mapping of data processing, can help mitigate these difficulties.

A comparison with the more mature and detailed European approach reveals the need for evolution in Brazilian regulations. The creation of specific regulations and the clear definition of eligibility criteria for the RIPD are fundamental steps to strengthen the protection of personal data in Brazil. With these measures, it is expected that data controllers will have greater legal certainty and clarity to fulfill their obligations and protect the rights of data subjects effectively.

Furthermore, it is essential that the National Data Protection Authority (ANPD) promote more objective guidelines and incentives for the adoption of good practices related to the RIPD. The creation of guidelines, the holding of public consultations, the publication of specific regulations on the subject and the encouragement of the exchange of experiences between data processing agents and the authority can contribute to the consolidation of a more uniform understanding on the subject. At the same time, organizations must invest in the training of their professionals and in the improvement of their data governance structures, ensuring that the RIPD is not just a formal requirement, but an effective instrument in risk management and in the protection of the privacy of data subjects. The evolution of the regulation and organizational culture surrounding the RIPD will be decisive for Brazil to reach a level of maturity compatible with the challenges and technological advances in the processing of personal data.

REFERENCES

ANPD (Autoridade Nacional de Proteção de Dados). 2022. *Resolution CD/ANPD No. 2, of January 27, 2022.* Gov.br. Accessed June 21, 2025. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022.

ANPD (Autoridade Nacional de Proteção de Dados). 2023a. *Personal Data Protection Impact Report (RIPD).* Gov.br. Accessed June 21, 2025. https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd.

ANPD (Autoridade Nacional de Proteção de Dados). 2023b. *Resolution CD/ANPD No. 11, of December 27, 2023.* Gov.br. Accessed June 21, 2025. https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-11-de-27-de-dezembro-de-2023-534947737.

ANPD (Autoridade Nacional de Proteção de Dados). 2024. *Public Consultation – Guidance on the Processing of High-Risk Personal Data.* Gov.br. Accessed June 21, 2025. https://www.gov.br/participamais brasil/blob/baixar/48651.

Article 29 Data Protection Working Party. 2017. *Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation (EU) 2016/679.* Accessed June 21, 2025. https://ec.europa.eu/ newsroom/article29/items/611236.

Barbosa, Elaine Muniz. 2016. "Integration of Social Network Data into Data Warehouses." Master's thesis, Federal University of Minas Gerais. Accessed June 21, 2025. http://hdl.handle.net/1843/ESBF-AKUNG3.

Brazil. 2018. *Lei No. 13.709, de 14 de Agosto de 2018 (Lei Geral de Proteção de Dados).* Accessed June 21, 2025. https://www.planalto.gov.br/ ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

Cabral, Filipe Fonteles. 2019. "The Personal Data Protection Impact Report as an Instrument for Risk Management in the General Personal Data Protection Law." In *Special Notebook: General Data Protection Law (PGPD)*, 200–211. São Paulo: Revista dos Tribunais.

Dozza, Eleonora Coelho. 2023. "Secondary Use of Personal Data and Its Basis in Legitimate Interest in Post-LGPD Brazil." https://lume.ufrgs.br/bitstream/handle/10183/264345/001173367.pdf.

European Data Protection Board. 2018. "Endorsement of the Working Party 29 Guidelines on GDPR by the EDPB." Accessed June 21, 2025. https://www.edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.

Gomes, Maria Cecília O. 2019. "Beyond a 'Legal Obligation': What the Benefits and Risks Methodology Teaches Us about the Data Protection Impact Report." In *Digital Law: Contemporary Debates*, edited by Ana Paula Lima, Carmina Hissa, and Paloma Mendes Saldanha, 141–153. São Paulo: Revista dos Tribunais.

Gomes, Maria Cecília. 2021. "Data Protection Impact Report: Mandatory for the Processing of Sensitive Data?" In *LGPD in Health*, edited by Analluza Bolivar Dallari and Gustavo Ferraz Monaco, 263–275. São Paulo: Thomson Reuters Brazil.

Gomes, Maria Cecília. 2022. "Data Protection Impact Report: A Brief Analysis of Its Definition and Role in the LGPD." Accessed June 21, 2025. https://mariaceciliagomes.com.br/wp-content/uploads/2022/01/ Relatorio_de_Impacto_a_Protecao_de_Dados.pdf.

Grasso, Ian Matiello. 2021. "Impact Report on the Protection of Personal Data in the General Data Protection Law: A Trivialization?" *Legal Notebooks of the Sorocaba Law School – Digital Law* 3 (1): 142–174.

LCNN (National Laboratory for Scientific Computing). 2024. "What Is Personal Data Mapping?" Gov.br. Accessed June 21, 2025. https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/gestao-de-seguranca-da-informacao/o-que-e-mapeamento-de-dados-pessoais.

Lohmann, Pedro A., and Raphael Carlos Albuquerque. 2021. "Systematic Review for the Data Protection and Privacy Impact Assessment Process." Unpublished manuscript.

Sturari, Matheus. 2020. "The DPIA in the LGPD: National Interpretation or Trivialization of the Instrument?" LinkedIn, July 22, 2020. Accessed June 21, 2025. https://www.linkedin.com/pulse/o-dpia-na-lgpd-interpretação-nacional-oubanalização-do-matheus/.

* * *

Rainier Garacis
Post-graduate in Digital Law from the Institute for Technology and Society of Rio de Janeiro, Brazil.
Email: r.garacis@hotmail.com
ORCID iD: https://orcid.org/0009-0003-9847-7842

10.59224/bjlti.v3i1.100-116
ISSN: 2965-1549