2023, April

Brazilian General Personal Data Protection Law (LGPD) and the Clarifications about the Data Protection Impact Assessment (DPIA)

Learn more about Brazilian Data Protection Authority (ANPD)'s answers to the main questions about the document focused on risk management in the treatment of personal data

TAUIL | CHEQUER
MAYER | BROWN

QUESTIONS

1 | When should the DPIA be prepared?

2 | What is considered “high risk” in the DPIA?

3 | What are the minimum requirements of the DPIA?

4 | What are the topics of a DPIA?

5 | What data and information should be included in the DPIA?

6 | Must the DPIA be public?

7 | What should be done after preparing the DPIA?

8 | What is the step-by-step for the elaboration of the DPIA?

WHEN SHOULD THE DPIA BE PREPARED?

TAUIL | CHEQUER
MAYER | BROWN

IT IS RECOMMENDED TO PREPARE THE DPIA:

Prior to any processing of data **(independent action of the data controller in attention to the principle of responsibility and accountability)**.

Em situações em que as operações de tratamento de dados pessoais possam representar alto risco à garantia dos princípios gerais de proteção de dados pessoais e às liberdades civis e aos direitos fundamentais do titular de dados – critérios que devem ser avaliados pelo agente de tratamento.

Por motivação ou **determinação da ANPD**.

Specific situations in which the DPIA may be required by the ANPD, such as: when the processing is based on legitimate interest or when it involves sensitive personal data.

Privacy governance program: the program must establish adequate safeguards based on a process of systematic assessment of privacy impacts and risks, a procedure that may involve the drafting of the

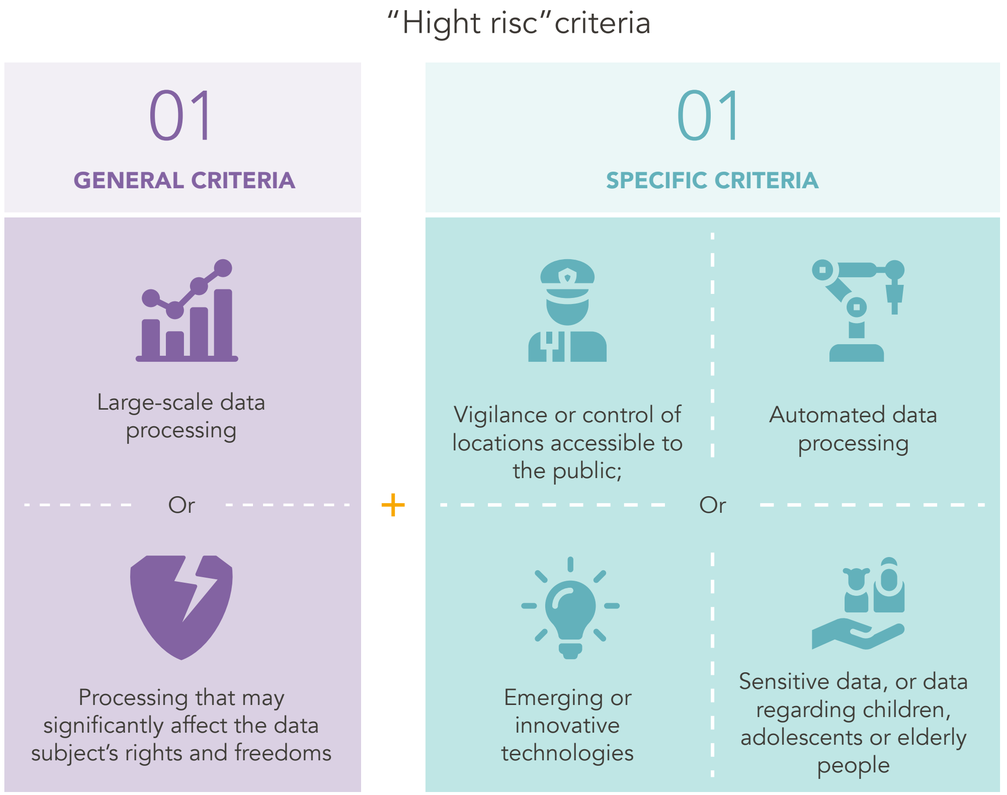
WHAT IS CONSIDERED "HIGH RISK" IN THE DPIA?

TAUIL | CHEQUER
MAYER | BROWN

ANPD has provided that until specific regulations are issued on the DPIA, controllers may, where applicable, **adopt as a parameter the concept of high-risk processing** defined in Article 4 of the LGPD's Regulation for the application of the LGPD for small processing agents.

- A personal data processing **will be considered high-risk if it meets at least one of the general criteria and one of the specific criteria**, as indicated in the image to the side – a scenario in which the preparation of a DPIA will be recommended.

These criteria are not exhaustive and the controller must evaluate the circumstances of each particular case to identify whether there are other criteria that could lead to a high risk to principles, freedoms or rights.ou direitos dos titulares.



DURING THE ELABORATION OF THE DPIA, IT IS IMPORTANT TO IDENTIFY:

- As many risk factors as possible and to estimate the likelihood of their materialization; and
- The impact of harm that may be caused to data subjects.

WHAT ARE THE MINIMUM REQUIREMENTS OF THE DPIA?

TAUIL | CHEQUER
MAYER | BROWN

Description of the categories of personal data collected or processed in any way;

Methodology used for processing and for ensuring information security; and

Controller analysis regarding measures, safeguards, and risk mitigation mechanisms adopted.

WHAT ARE THE TOPICS OF A DPIA?

TAUIL | CHEQUER
MAYER | BROWN

- Description of the categories of personal data processed;
- Name of the processing operations;
- Purposes of processing (including legitimate interests);
- Legal basis adopted;
- Assessment of the necessity and proportionality of the processing operations;
- Analysis of risks to the rights and freedoms of data subjects; and
- Measures to be taken to minimize these risks.

In any case, ANPD may request additional information, whenever necessary.

WHAT DATA AND INFORMATION SHOULD BE INCLUDED IN THE DPIA?

TAUIL | CHEQUER
MAYER | BROWN

A. a. Identification of the processing agents and the data protection officer;

B. b. Other interested/involved parties. Inform if they were consulted in the preparation of the DPIA and opinions issued;

C. c. Justification for the need to prepare the assessment (for example: high risk, ANPD request, risk management and prevention, others);

D. d. Project/Process that justifies the preparation of the DPIA;

E. e. Information systems related to the project/ process that justifies the preparation of the DPIA;

F. f. Data processing, including:

- Description of the processing (from collection to disposal);
- Personal data (provide full details of all categories of personal data processed);
- Sensitive personal data (provide all categories of sensitive personal data processed, in full);
- Categories of data subjects (e.g., customers, controller's employees, children of controller's employees, customer's employees, plaintiffs, policy beneficiaries, third party service providers)
- Data of children and adolescents or other vulnerable category, such as the elderly, if any;
- Volume of personal data processed and number of data subjects involved in processing;
- Source of collection;
- Purpose of processing (Justify the purpose of processing for each data);
- Inform about internal and external sharing (including international transfer, if any); and
- Storage policy (describe the retention periods and disposal methods).

G. Legal hypothesis analysis. Justify the choice of legal hypothesis for each processing purpose;

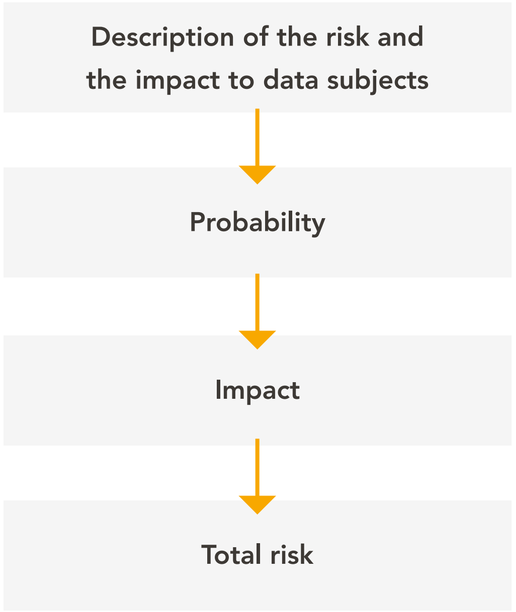
H. Analysis of LGPD principles;

I. Identified risks to the data subject;

WHAT DATA AND INFORMATION SHOULD BE INCLUDED IN THE DPIA?

TAUIL | CHEQUER
MAYER | BROWN

J. Outcome calculated based on the methodology used by the processing agent:



K. Measures, safeguards and risk mitigation mechanisms:

*Describe the measures adopted to mitigate the risk.

MUST THE DPIA BE PUBLIC?

Although not mandatory, the ANPD recommends that private entities make the DPIA public as a measure that **demonstrates the controller's concern with personal data security and its commitment to the data subjects' privacy**, meeting the principles of transparency and accountability provided in the LGPD.

The controller may make the DPIA available in means of easy access to the data subject, such as on its websites, provided that commercial secrets and information protected by law are safeguarded.

PUBLIC ENTITIES

In the case of public entities, the DPIA must be published by determination of the ANPD or by the controller itself, in accordance with Law No. 12.527 of 2011.

WHAT SHOULD BE DONE AFTER PREPARING THE DPIA?

TAUIL | CHEQUER
MAYER | BROWN

After preparing the DPIA, the controller will **verify whether or not it is viable to continue with the personal data processing** that prompted the assessment or whether a change in the form of processing is required.

The processing agent will observe the recommendations coming from the DPIA, especially regarding **the implementation of measures, safeguards and risk mitigation mechanisms adopted**.

Finally, it is recommended to the controller to **continuously review the DPIA**, especially when there are new facts that may lead to changes in the identified risks, such as:

- Changes in the processing operations.
- Identification of new risk factors.
- Aggravation of previously identified risk factors.
- In case of new regulations or guidelines issued by the ANPD.

WHAT IS THE STEP-BY-STEP FOR THE ELABORATION OF THE DPIA?

TAUIL | CHEQUER
MAYER | BROWN

DPIA

Data Processing Impact Assessment