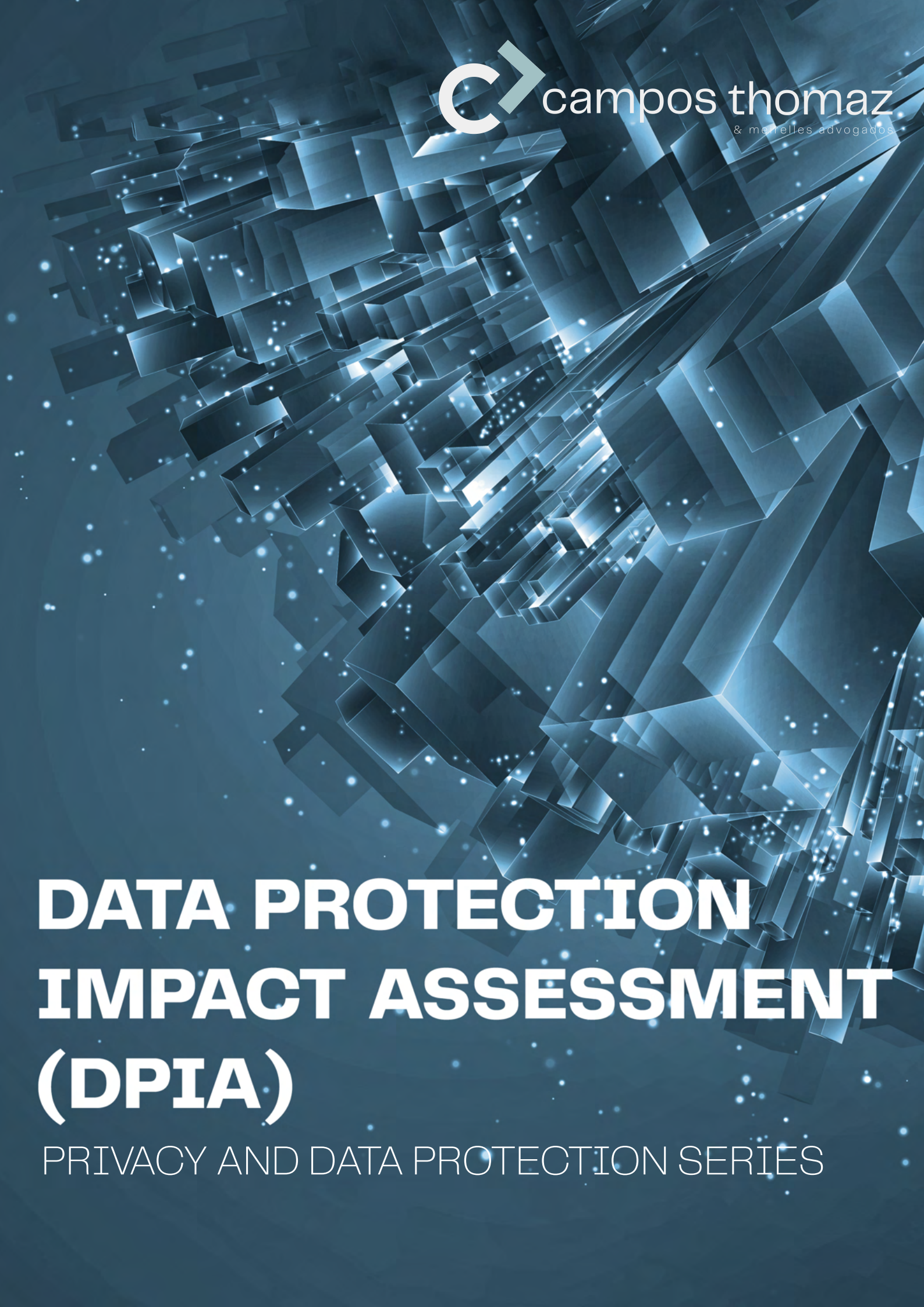

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

PRIVACY AND DATA PROTECTION SERIES

TABLE OF CONTENTS:

1

What is a DPIA and what is its objective?

DPIA stands for "Data Protection Impact Assessment", which is one of the requirements of the Brazilian General Data Protection Law ("LGPD"[1]). This is a document required from the data controller, who is responsible for making decisions about how personal data will be processed, including the definition of the type of data, and the purpose of the processing.

The DPIA must describe the personal data processing activities that may represent risks to civil liberties and fundamental rights. It must also provide for measures, safeguards, and mechanisms to mitigate these risks[2]. Although the DPIA's preparation is recommended mainly for data processing activities with high risk to data subjects, it is crucial to consider it for any other data processing activity with a large amount of personal data, such as profiling, sensitive personal data, and data of vulnerable data subjects.

The DPIA aims to assess the risks of a particular personal data processing activity and define measures to mitigate the identified risks. Also, this is a document that the Brazilian Data Protection Authority ("ANPD") may request at any time, therefore, organizations must have it for the data processing activities mentioned above (i.e., high-risk personal data processing activities, data processing activities involving a large amount of personal data, sensitive personal data, or data of vulnerable data subjects).

Preparing the DPIA is a legal requirement and a good risk management practice for organizations. That is because, in addition to avoiding sanctions and fines from the ANPD, it helps to ensure the trust of data subjects and relevant business partners.

[1] LGPD, Article 38. The Brazilian Data Protection Authority may determine that the controller prepare a Data Protection Impact Assessment, including sensitive data related to its data processing operations, following regulations, subject to commercial and industrial secrecy.

[2] LGPD, Article 5, item XVII. "Data Protection Impact Assessment: documentation of the controller containing a description of the personal data processing activities that may pose risks to civil liberties and fundamental rights, as well as measures, safeguards, and mechanisms for risk mitigation."

2

How to identify the need for developing a DPIA?

As provided for by the LGPD, the scenarios in which the ANPD may request the DPIA are:

When the data processing activity has a legitimate interest as its legal basis[3].

At any time under the ANPD's requirement[4].

However, at the end of 2020, the "Digital Government Secretariat of the Special Secretariat for Debureaucratization, Management, and Digital Government of the Ministry of Economy" (in Portuguese, “Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia”) published a "DPIA Guide and Template"[5] ("Guide") that provides for situations in which the DPIA should be prepared, as follows:

- Use of new technology, service, or another new initiative in which personal data and sensitive personal data are or should be processed;
- Track of the location of individuals or any other processing activity that aims to form a behavioral profile;
- Processing of sensitive personal data;
- Processing of personal data for automated decision-making that may have legal effects, including decisions aimed at defining a person, professional, consumer, and credit profile, or even aspects of an individual's personality;
- Processing of data of children and adolescents;
- Processing of data that may result in some pecuniary, moral, individual, or collective damage to data subjects in case of information security incidents;
- Processing of personal data carried out for the exclusive purpose of public security, national defense, State security, or investigation and repression of criminal offenses;
- Processing of personal data based on the controller's legitimate interest;
- Changes in laws and regulations applicable to data protection, or even in internal policies and information system, alteration of data flows, and
- Administrative reforms that imply a new organizational structure resulting from agencies or entities' merger, consolidation, or spin-off.

In summary, it is ideal for organizations to prepare a DPIA before beginning any high-risk data processing activity to evaluate potential risks to data subjects. Additionally, DPIAs should be considered for any other procedures involving the processing personal data at a large scale, using innovative solutions, creating and defining profiles, handling sensitive personal data, or dealing with data of vulnerable data subjects.[6]

[3] LGPD, Article 10, item II, § 3.
[4] LGPD, Article 32.
[5] Available at: <Guia e Template: Relatório de Impacto à Proteção de Dados Pessoais>. Accessed on March 15, 2023.
[6] EUROPEAN COMISSION. Guidelines on Data Protection Impact Assessment (DPIA). Available at: <https://ec.europa.eu/newsroom/article29/items/611236/en>. Accessed on: March, 15 2023.

3

The Privacy by Design in a DPIA

The "Privacy by Design" model was first published in 1995 in a joint report by Ann Cavoukian, the model's author, and John Borking of the Dutch Data Protection Authority. In 2010, the model was recognized as essential for privacy protection and gained prominence in various privacy and data protection guidance models worldwide.

The DPIA aligned with Privacy by Design aims to analyze risks and prevent potential privacy violations from the start of a personal data processing activity in a business. Thus, it takes a preventive approach rather than just a corrective one.

Combining the DPIA with Privacy by Design allows for a comprehensive description of the processes of a personal data processing activity from its inception, including the assessment of potential risks and prevention measures related to the processing activity. As the DPIA essentially addresses data processing with high risk to data subjects, Privacy by Design is crucial for the responsible and safe use of personal data, assisting in the elaboration and implementation of the DPIA.

4

What aspects should be addressed in a DPIA?

According to article 38, sole paragraph of the LGPD, a DPIA must have at least the following items:

I.
Description of the types of data collected;

II.
Methodology used for data collection and information security guarantee; and

III.
Controller's analysis regarding the measures, safeguards, and mechanisms for risk mitigation adopted.

Although the LGPD provides for the elaboration of the DPIA, the subject will still be further regulated by the ANPD, as provided for in its regulatory agenda. However, the federal government has already made available the Guide, which can assist data controllers and their Data Protection Officers ("DPOs") in elaborating a DPIA.

Moreover, organizations must follow the rules and guidelines of the LGPD when using the legal basis of legitimate interest to process personal data.

In summary, the Guide provides for eight steps for the elaboration of a DPIA, which are:

1. IDENTIFICATION OF THE DATA PROCESSING AGENTS AND DPO

Identification of the controller, processor, and DPO in the DPIA, including the DPO's email and phone contact, as they are the communication channel between the controller, data subjects, and the ANPD.

2. NEED FOR THE ELABORATION OF THE DPIA

The organization must evaluate whether it is necessary to prepare a DPIA and, if so, whether a single DPIA will be prepared for all data processing activities or a DPIA for each project.

The organization itself must internally evaluate the adequacy above. Suppose it is an organization with several projects, services, and systems with significant data processing. In that case, it should opt for the elaboration of separate DPIAs. If it is an organization with few data processing activities, it may opt for elaborating a single DPIA.

The evaluation should also consider cases where the DPIA should or can be requested by the ANPD and in the hypotheses listed in Item 2.

3. DESCRIPTION OF PERSONAL DATA PROCESSING

NATURE

How the organization carries out or intends to carry out data processing activities, describing how personal data is collected, stored, processed, used, and deleted; the data source; whether there is sharing and with which organizations data is shared; the processors involved and at what stage of processing; whether there is the use of new technologies that may increase the risk of data leakage; and the security measures adopted to protect this data.

SCOPE

The extent of the organization's data processing, describing the types of personal data processed, specifying whether there is sensitive personal data, the volume of data collected and processed, the quantity and frequency of processing, the retention period, the number of affected data subjects, and the geographic scope of the processing.

CONTEXT

identification of what factors, internal and external to the organization, may impact data processing and the data subject's expectations, describing the nature of the controller's relationship with the data subject; the level/method of control that the data subject has over their data; whether the processing is aligned with the data subject's expectation and disclosed purpose; the controller's previous experience in this type of processing; and the organization's technological and security advances that may contribute to the protection of personal data.

PURPOSE

the reason for the desired processing to justify the processing and inform the data subject, according to the hypotheses contained in articles 7 and 11 of the LGPD. It is essential to indicate the intended processing results for the data subject and the expected benefits for the organization, entity, or society.

4. AGENTS OR STAKEHOLDERS INVOLVED IN THE DATA PROCESSING ACTIVITY

List all those consulted about personal data that is or will be subject to processing, such as the processor, DPO, managers, information security experts, and legal consultants. It is also necessary to list each party's opinion regarding data processing risks.

5. NEED AND PROPORTIONALITY

Demonstrate if the collected data is limited to the minimum necessary to achieve the proposed purpose, being relevant, proportional, and not excessive. It is important to ensure data quality, accuracy, clarity, relevance, and update, and describe the measures to meet data subjects' rights.

6. IDENTIFICATION AND RISK ASSESSMENT

Identify the risks that could potentially impact data subjects by creating a risk matrix that lists all types of risks involved in the processing of personal data. The matrix should also include measures, safeguards, and mechanisms to mitigate identified risks.

7. MEASURES USED TO COLLECT AND PROTECT PERSONAL DATA AND RISK TREATMENT

As provided for in the LGPD, data processing agents must adopt technical and administrative measures capable of protecting personal data from unauthorized access and accidental or illicit situations of destruction, loss, alteration, communication, or any form of inadequate or illicit processing.[7]

The organization must have in mind security and privacy processes and solutions to remain in compliance with the LGPD, as well as list the applicable measures for the treatment of each potential risk in the processing of data from the data subjects.

8. APPROVAL BY THE RESPONSIBLE PARTIES

This is the stage where the DPIA needs to be formalized through the signatures of those responsible for approving the document: (a) the representative of the controller, (b) the representative of the processor, (c) the DPO, and (d) the person responsible for preparing the report.

9. REVIEW

It is relevant that the organization is attentive to the DPIA review procedures, considering the dynamism of an organization's operations and businesses and the continuous evaluation of personal data processing activities.

[7] LGPD, Article 46.

5 The importance of elaborating a DPIA and how Campos Thomaz & Meirelles Advogados can help you

The elaboration of the DPIA is an opportunity for the organization to assess its level of compliance with the LGPD and demonstrate its commitment to privacy and personal data protection, before data subjects and the ANPD. Thus, the organization also demonstrates its commitment to the principle of accountability, complying with data protection regulations and demonstrating the effectiveness of all applied measures.

Campos Thomaz & Meirelles Advogados offer comprehensive advice for compliance with the LGPD and all requirements related to privacy and personal data protection legislation.

Our recognitions

Análise Advocacia (2021)

Chambers & Partners Brazil (2021 & 2022)

Leaders League (2021 & 2022)

Transactional Track Record (2021 & 2022)

The Legal 500 (2022)

Meet our Partners

Alan Campos Thomaz

Partner

Technology & Digital Business, Privacy and Data Protection, Fintechs and Intellectual Property

at@camposthomaz.com

+55 11 9 8375.2627 +1 (650) 6436652

Sérgio Meirelles

Partner

Corporate, M&A, Venture Capital and Wealth

sergio@camposthomaz.com

+55 11 9 7551.9865

Filipe Starzynski

Partner

Litigation & Law Enforcement, Civil, Real State, Labor and Family

filipe@camposthomaz.com

+55 11 9 7151.9639

Juliana Sene Ikeda

Partner

Intellectual Property, Technology, Contracts and Life Sciences

juliana@camposthomaz.com

+55 11 9 8644.1613

Follow us

campos thomaz & meirelles advogados

Subscribe to our newsletter