

LGPD COMPLIANCE

To ensure compliance with the obligations established by the General Data Protection Law ([Law No. 13,709/2018 - LGPD](#)), make sure to fulfill all the items on this checklist.

☐

Evaluate the need to appoint a DPO.

Is it necessary to appoint a DPO? For more details, refer to the [CHECKLIST | COMPLIANCE WITH THE DPO REGULATION](#).

Note: The obligation to appoint a DPO does not apply to small-scale data processing agents, according to the rules established in [Resolution CD/ANPD No. 2/2022](#). Nevertheless, the ANPD considers the appointment of a DPO, even in cases of exemption, as a good governance practice.

☐

Raise awareness about the importance of the topic.

Is the company familiar with the current regulations and the compliance process? Are employees aware that the LGPD should guide all activities involving personal data?

☐

Map and record activities that involve the processing of personal data.

Are the company's activities involving the processing of personal data properly identified and recorded in an organized manner? Has the applicable legal basis been assigned to each mapped activity? For more details, please refer to the [DATA MAPPING TEMPLATE](#).

☐

Assess the recorded activities and identify areas for improvement.

Are the activities in compliance with the legislation? Is there any violation or high risks of non-compliance with regulatory requirements or infringement of data subjects' rights? Considering the company's business model, what areas can be improved?

☐

Review strategic contracts.

Do the contracts identify the purposes of personal data processing activities? Do the contracts establish limits for data processing carried out by third parties? What is the level of criticality and risk of the activities? For more details, please refer to the [CHECKLIST | CONTRACT NEGOTIATION](#).

☐**Implement a communication channel with data subjects and the ANPD.**

Is the channel available in a visible and easily accessible location for interested parties? Does the channel enable the receipt, analysis, response, and recording of communications?

☐**Implement transparency measures.**

Does the company provide clear, accurate, and easily accessible information about how personal data is used? Is the information organized considering the type of data subject the company interacts with?

☐**Implement governance procedures and policies.**

Have procedures and policies been defined to ensure an effective data protection governance program? Are employees aware of these procedures and policies? Are tools implemented to monitor and ensure the effectiveness of the measures adopted?

☐**Implement risk assessment mechanisms.**

Are there mechanisms in place to identify risks in activities involving the processing of personal data? Are activities with identified risks evaluated through a Data Protection Impact Assessment (DPIA)? For activities grounded on the legal basis of legitimate interest (Art. 7, IX, of the LGPD), is there a structured procedure for conducting a Legitimate Interest Assessment (LIA)?

☐**Evaluate international data transfers.**

Does the company have procedures to assess international data transfers? Have the destination locations and third parties involved been identified? Have safeguards been established to support these transfer activities?

☐**Implement security measures.**

Are technical and administrative measures adopted to protect personal data? Have procedures been defined for handling security incidents? Are these measures regularly reviewed and updated?

☐**Define data retention and disposal rules.**

Have the retention periods been defined and the reasons for retaining personal data documented? Are there procedures outlining the method of data disposal after the retention period has ended?