



DATA PROTECTION GOVERNANCE PROGRAM POLICIES

A successful data protection governance program requires the establishment of rules and procedures to ensure compliance with the obligations set forth by the General Data Protection Law ([Law No. 13.709/2018 - LGPD](#)) and to demonstrate the company's commitment to data subjects, business partners, and authorities.

Depending on the company's business model, specific measures may be necessary or recommended. However, the checklist below outlines some important policies for creating a data protection governance program aligned with the applicable law.



Privacy Policy

External document intended to inform data subjects with whom the company interacts about: **(i)** purposes of data processing; **(ii)** data subjects' rights and how to exercise them; **(iii)** information security practices adopted; **(iv)** data sharing practices; **(v)** duration of data processing activities, among other topics. The Privacy Policy must be made available in a visible and easily accessible location, using clear and simple language.



Cookie Policy

A policy typically applicable to websites, applications, and software, providing information on the use of cookies and/or similar technologies, and explaining to data subjects how such technologies are used in activities involving personal data. This policy should follow the same requirements as the Privacy Policy but with a specific focus.



Information Security Policy

Policy that establishes the strategies and parameters adopted to protect information assets and personal data processed in the company's activities.



Security Incident Response Policy

Document that sets out the rules, roles, and responsibilities for managing security incidents, including specific procedures to be followed in the event of a confirmed incident or even a suspected incident. This policy should also include procedures for assessing and notifying data subjects and the National Data Protection Authority (ANPD), as applicable.



Human Resources Privacy Policy

A policy similar to the Privacy Policy, but with an internal focus, aimed at the company’s employees, and designed to clarify how their personal data is processed by the company for the maintenance of the employment relationship.



Supplier Contracting Policy

Document that defines the procedures for analyzing, selecting, contracting, and monitoring suppliers who will process personal data as part of their relationship with the company. The outlined procedures should allow for an assessment of the supplier’s data protection governance program maturity level.



Data Subjects’ Rights Policy

Policy that establishes communication channels, responsible teams, internal workflows, and procedures for receiving, recording, and responding to data subject rights requests presented by data subjects.



Data Retention and Disposal Policy

Policy that outlines the guidelines for determining the retention period of personal data, including applicable legal grounds, and the procedures to be followed for disposing of data after the retention period has ended.



Data Protection Governance Policy

Document that consolidates the company’s practices and procedures related to data protection, defining the guidelines that must be followed in all activities involving personal data. This document may include the definition of situations that require the preparation of a Data Protection Impact Assessment (DPIA) and a Legitimate Interest Assessment (LIA), as well as other tools used to identify and evaluate risks in the company’s activities.