

# DATA PROTECTION GOVERNANCE PROGRAM KPIs



## How to measure the effectiveness of the program?

Assigning metrics to the data protection governance program is important for closely monitoring the progress of activities, with indicators highlighting areas of strength or those that require improvement.

**KPIs allow:**

- ☒ Evaluate the effectiveness of the adopted practices
- ☒ Identify deficiencies and associated risks
- ☒ Continuously monitor compliance
- ☒ Support strategic decision-making

With this scenario in mind, **b/luz** has developed a practical guide that outlines some steps the DPO can follow to manage metrics associated with a data protection governance program.

## FIRST STEP | Ensure that the program is minimally structured

A structured program provides a solid foundation for the continuous measurement and management of data protection practices. This is essential for implementing and managing effective metrics.

In this first step, aim to answer the following questions:

- **Roles and responsibilities:** who are the individuals responsible for data protection matters within the organization? What are the strategic areas of the organization? Are there means to ensure the collaboration of these individuals?
- **Procedures and policies:** are there procedures and policies that minimally structure the data protection governance program? Are employees aware of these procedures and policies?

**For more information on how to structure a data protection governance program, visit:**

- [Checklist | LGPD Compliance](#)
- [Checklist | Policies](#)

## SECOND STEP | Parametrize the program’s measurement pillars

To ensure effective management of the program, aim to structure at least the following points:

- **Measurement pillars:** fundamental axes of the program that will guide continuous evaluation and management.
- **Performance indicators:** metrics and criteria that will allow the assessment of whether the program is progressing in the right direction. These indicators will help monitor progress, identify areas that need adjustment, and ensure that goals are being achieved.

*For example:*

| Pillars                                                                                                  | KPIs                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RECORD OF ACTIVITIES</b><br><br>Documentation and monitoring of the processing activities carried out | <ul style="list-style-type: none"><li>• Total number of activities mapped in each registration cycle</li><li>• Average volume of new activities mapped per month or year</li><li>• Average frequency at which mapped activities undergo changes</li><li>• Average time it takes for departments to complete the records</li><li>• Average time to review the records</li></ul> |

|                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>AWARENESS</b></p> <p>Ongoing training and education of employees on data protection practices</p>                             | <ul style="list-style-type: none"><li>• Number of training sessions conducted</li><li>• Amount of awareness content produced</li><li>• Audience reach</li><li>• Results of evaluations or knowledge tests conducted</li><li>• Employee feedback on the clarity and usefulness of the provided content</li></ul>                                          |
| <p><b>RISK MANAGEMENT</b></p> <p>Identification, assessment, and mitigation of risks associated with data processing activities</p> | <ul style="list-style-type: none"><li>• Number of high-risk processing activities identified</li><li>• Quantity and level of risks mitigated in processing activities</li><li>• Number of security vulnerabilities identified and fixed before causing incidents</li><li>• Percentage of accepted risks</li><li>• Percentage of residual risks</li></ul> |
| <p><b>DATA SUBJECTS' RIGHTS</b></p> <p>Management of rights requests submitted by data subjects</p>                                 | <ul style="list-style-type: none"><li>• Number of requests received</li><li>• Average response time</li><li>• Percentage of requests fully addressed</li><li>• Satisfaction rate of data subjects with the request handling process</li><li>• Categories of rights most requested and fulfilled</li></ul>                                                |
| <p><b>THIRD-PARTY MANAGEMENT</b></p> <p>Oversight and control of vendors and partners who process personal data</p>                 | <ul style="list-style-type: none"><li>• Number of contracts reviewed</li><li>• Average review time</li><li>• Number of adjustments made</li><li>• Average negotiation time</li><li>• Number of data protection due diligence processes conducted with vendors and partners</li></ul>                                                                     |
| <p><b>INCIDENTS MANAGEMENT</b></p> <p>Identification and response to security incidents</p>                                         | <ul style="list-style-type: none"><li>• Number of incidents investigated</li><li>• Number of incidents resolved</li><li>• Percentage of incidents reported to the ANPD and data subjects</li><li>• Average resolution time</li></ul>                                                                                                                     |

**THIRD STEP | Collect information and perform the necessary analyses**

This step involves applying the defined indicators to evaluate the effectiveness of the pillars of the data protection governance program. This step is crucial for obtaining real data on the program's performance, identifying areas that need improvement, and ensuring that established goals can be achieved.

- **Define sources:** identify all sources of information necessary to measure each defined KPI. This may include internal systems, reports, monitoring tools, and team feedback.
- **Define frequency:** establish how often the information should be collected (e.g., weekly, monthly, or annually) according to the requirements of each KPI.
- **Identify patterns and trends:** look for patterns and trends in the data to understand the overall performance of the program and identify recurring issues.

**FOURTH STEP | Adjust metrics and processes**

As the organization's needs evolve and the regulatory environment changes, it may be necessary to review and adapt the pillars, KPIs, processes, and objectives to ensure the program continues to meet the company's expectations and comply with legal requirements.

It is important that this analysis is performed periodically to ensure the effectiveness of the methodology – for example, annually.