Profile DPO Brasil 2025

Opice Blum

Rede Líderes

Index

Introduction

With the approval of the General Personal Data Protection Law (Federal Law nº 13,709/2018 - LGPD), organizations in Brazil faced new challenges and opportunities, and the Data Protection Officer (DPO) gained prominence as an essential figure in conducting adequacy strategies and maintaining compliance. The regulatory framework in Brazil also has supplementary regulation by the Brazilian National Data Protection Authority (ANPD) with the publishing of Resolution CD/ANPD No. 18/2024, which establishes rules for the DPO's activities, and of a guidance on this role.

Given this scenario, we present the **Report Profile DPO Brazil 2025**, a unique study that seeks to investigate the specificities of this professional's role, exploring the obstacles faced, the best practices adopted, and the impact of their work. The data presented aims to provide a practical and informative guide for organizations and professionals working in this market.

The survey was conducted between June and August 2025, with the selected and qualified participation of 203 professionals from various sectors and company sizes, who responded to a 23-question questionnaire. The results presented in this survey consider percentages without decimals based on valid and complete responses.

Executive Summary

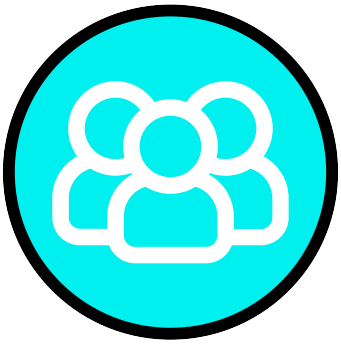
Browse the links to view the research results according to the following themes:

1. **Key takeaways:** main insights learned from the research
2. **Respondent profile:** survey qualification in relation to the target audience
3. **Profile of the DPO:** aspects that make up the figure of the DPO at the time of the research
4. **Structure and resources:** relationship between the DPO and the organization to perform the function
5. **Day-to-day:** activities and challenges faced in the daily work of the DPO
6. **Governance:** aspects of formal compliance and perception of maturity and risk
7. **Sectors:** exemplary sectoral comparison, with the main highlights of the research

Key takeaways

Exclusive dedication

Only 27% of the DPOs work exclusively in this role, and among those who perform other roles, 48% are in the Legal or Compliance department.

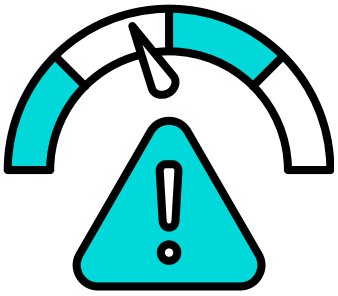


Teamwork

22% of the DPOs responded that they work alone in their organizations, while 69% stated that they have a dedicated privacy team of up to 5 people, a number that presents a great disparity in the international scenario, which, on average, reveals teams of 26 to 31 people.

Investment potential

While in Brazil, 74% of DPOs from companies with more than 1,000 employees have less than R$600,000 per year for this purpose, global companies of the same size invest, on average, between US$1 million and US$7 million annually in data protection.



Governance

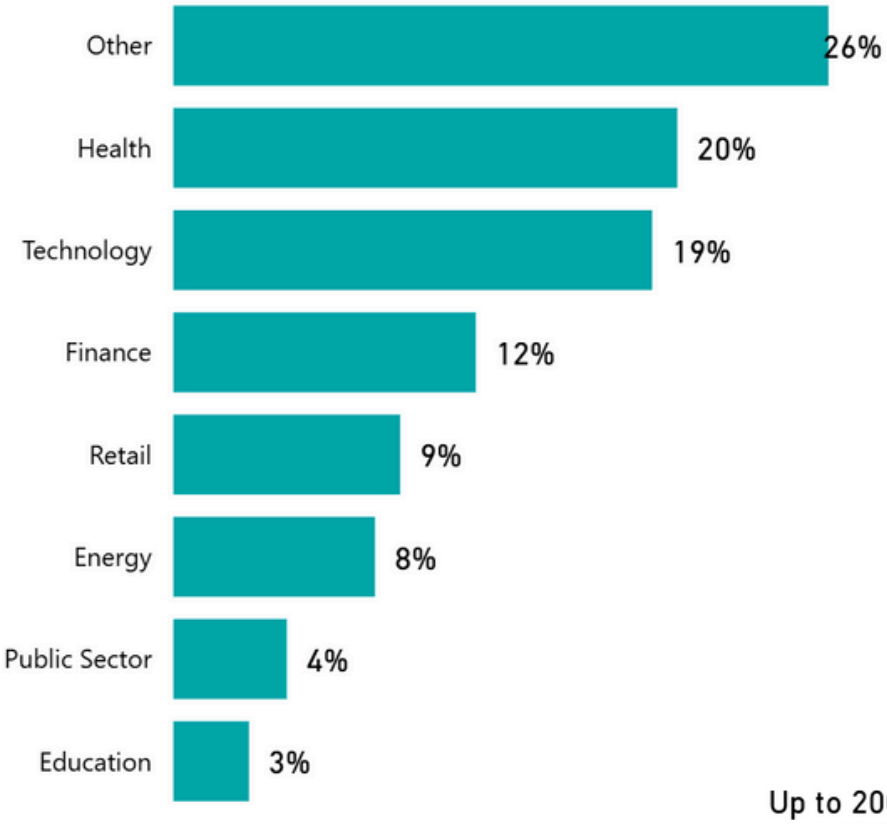
63% of the DPOs believe their organization has achieved a high or very high level of maturity in their data protection governance. However, 21% rate their maturity as low or medium, even though they perform high or very high-risk activities.

Back to index

Respondent profile

The respondents were DPOs from various sectors and sizes of organizations. The selected and qualified group was primarily internal DPOs.

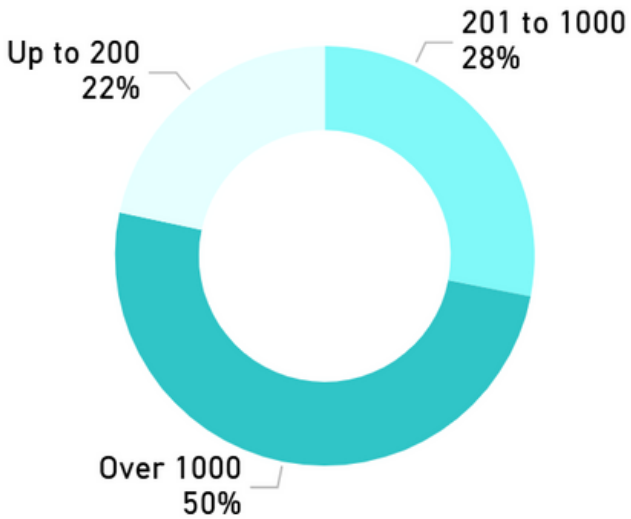
Sector of activity



The sectors with the highest participation were Healthcare (20%), Technology (19%), and Finance (12%). Also notable were the Energy (8%) and Public Sectors (4%), demonstrating a greater presence of the topic in regulated sectors. The "Other" category (26%) includes sectors not detailed in the survey, such as Automotive, Consulting, Communications, Tourism, and Real Estate.

Size of the organization

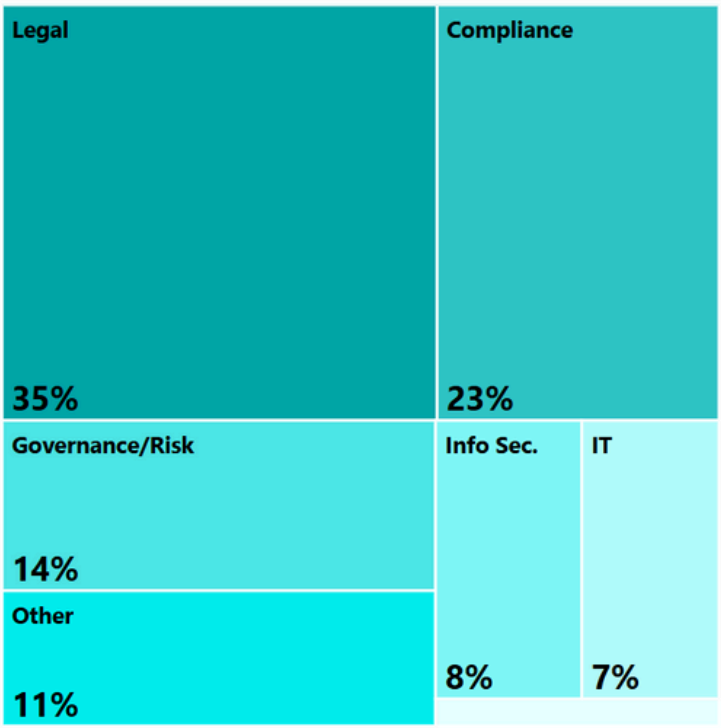
50% of respondents are from companies with more than 1000 employees.



Back to index

Profile of the DPO

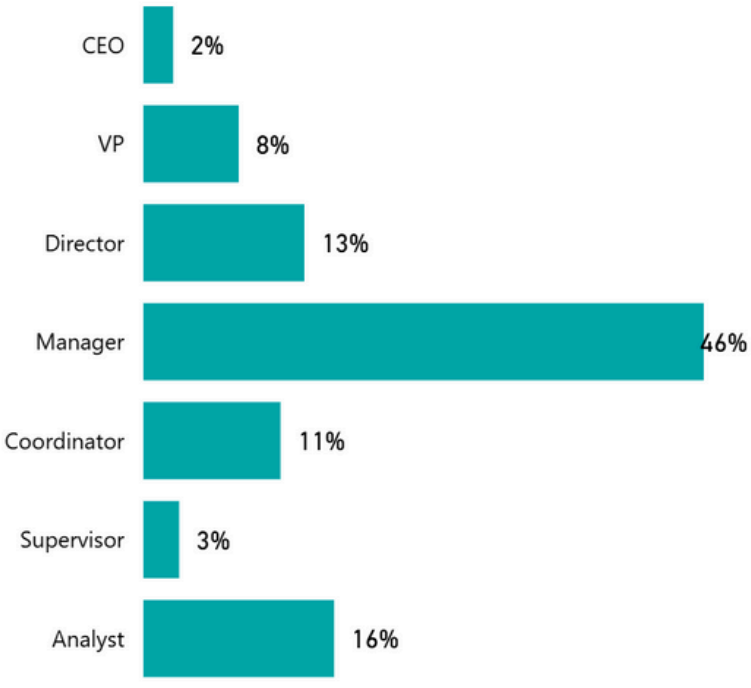
Where the DPO is located



DPOs are assigned to key areas of the organization, such as Legal, Compliance, and Governance/Risk, representing 72% of respondents. Technology-related areas also had a significant presence, with 15% of respondents assigned to Information Security or Information Technology. [1] The data aligns with the international scenario, which reveals the allocation of DPOs to sectors such as Legal (41%), Compliance (22%), and Information Security (13%).

What position does the DPO assume?

Regarding the hierarchical level of the DPO, there is a predominance of allocation to Management positions (46%). And at least 24% of respondents hold a Director position or higher, which contrasts with the international scenario, [2] where this position reaches 83%.



80% of CEOs who take on the role of DPO are in companies with fewer than 1,000 employees.

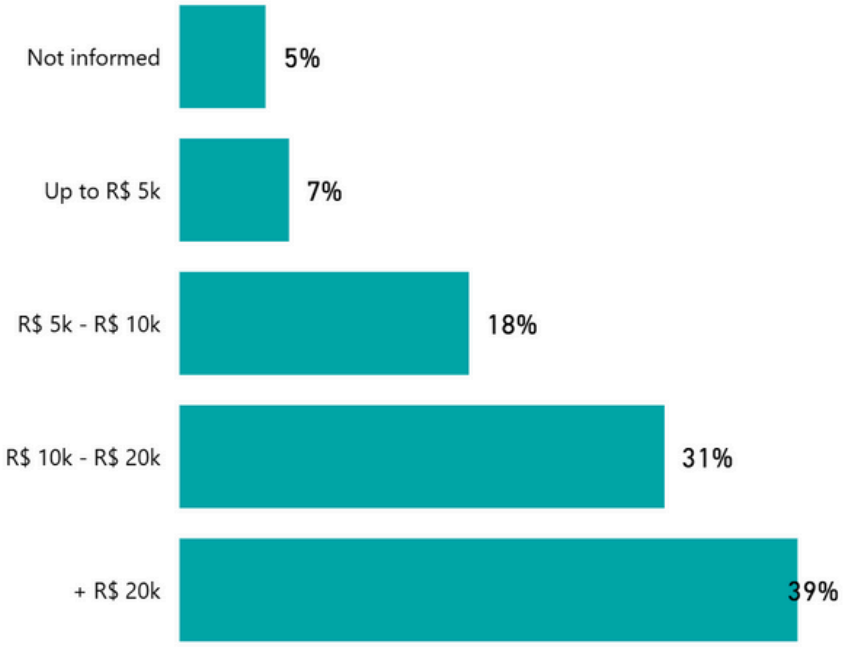
Back to index

[1] IAPP and EY's "Annual Privacy Governance Report 2022" (p. 19) available here
[2] IAPP Privacy Governance Report 2024 (p.30) available here

Profile of the DPO

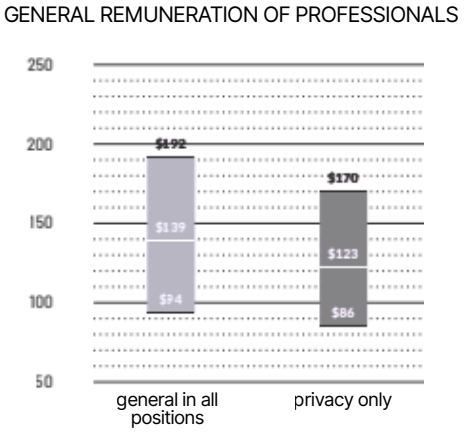
Monthly remuneration

69% of respondents have a monthly salary above R$10,000.00, reaching 76% when the Technology sector is analyzed isolated.



International comparison [3]

This compensation differs from the international scenario, where Data Protection Officers receive annual compensation ranging from $86,000.00 to $170,000.00 (as shown in the graph on the side)—which would correspond to $7,166.66 to $14,166.00 per month. A relevant factor for comparison is the possibility of combining functions or remuneration corresponding to the DPO's primary position.



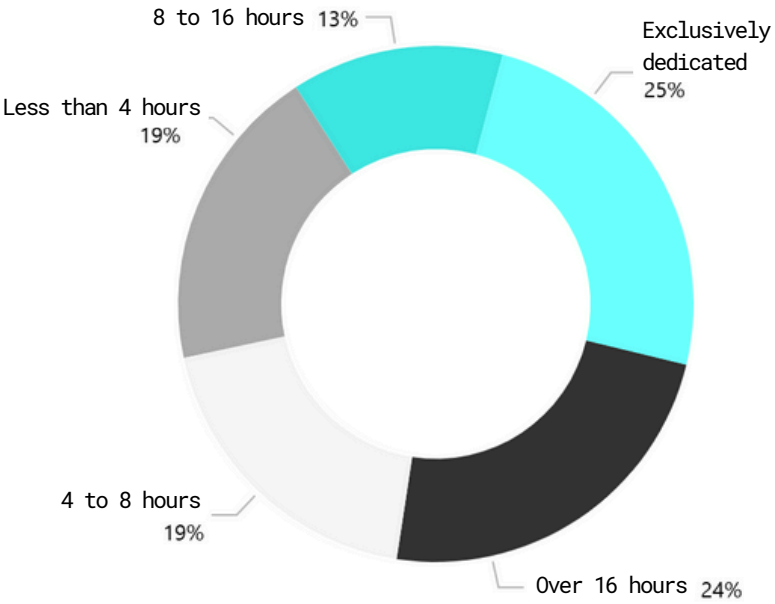
Back to index

[3] Salary and Jobs Report 2025–26 Privacy, AI Governance and Digital Responsibility, IAPP (p. 7), available here.

Structure and resources

The structure in which the DPO is inserted is a determining factor for their performance, impacting everything from the time dedicated to their level of autonomy in carrying out the function.

Weekly hours dedicated to the role

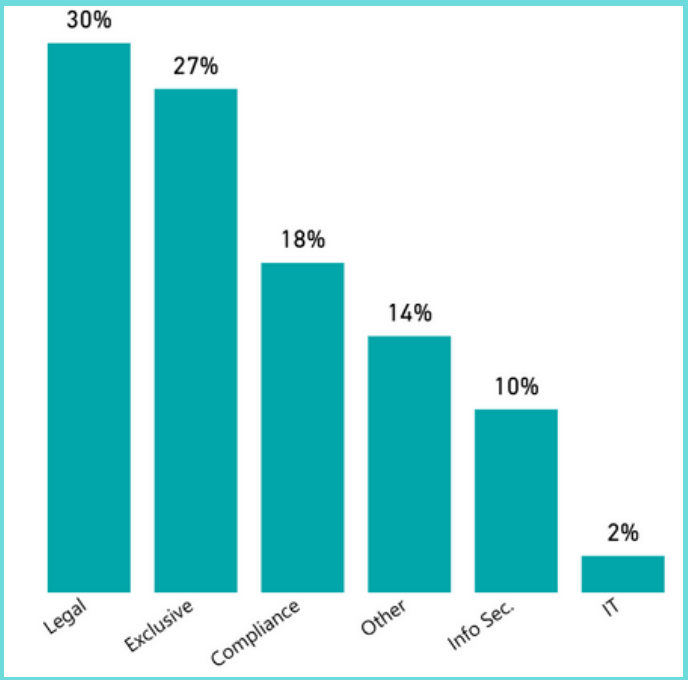


49% of respondents dedicate at least 16 hours per week or are exclusively dedicated to the role of DPO.

The data is consistent with the international scenario[4], in which an average of 46% of DPOs are exclusively dedicated to the role.

27% **act exclusively as DPO**

Among those who hold other roles, 48% work in regulatory departments (Legal and Compliance), while 12% work in technology departments (Information Security and IT). Other roles mentioned include ethics, anti-fraud, ombudsman, and risk management.



Back to index

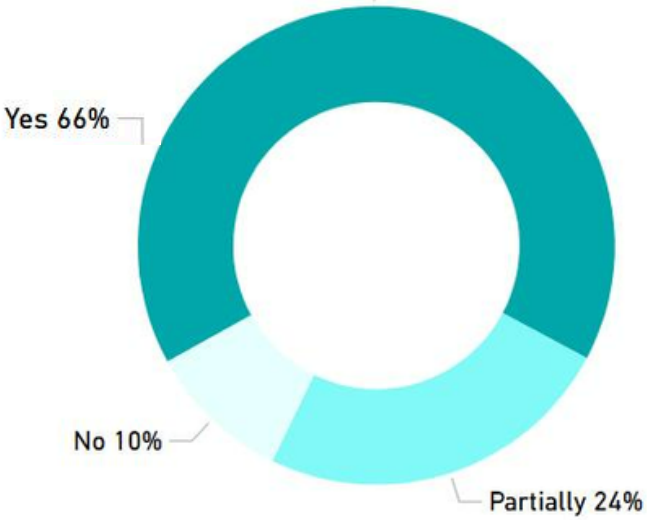
[4] Designation and Position of Data Protection Officers, EDPB 2024 (p.24), available here.

Structure and resources

Functional autonomy reflects the structure in which the DPO operates. This includes having the authority to report directly to senior leadership, not receiving instructions on how to perform these tasks, and not having conflicts of interest.

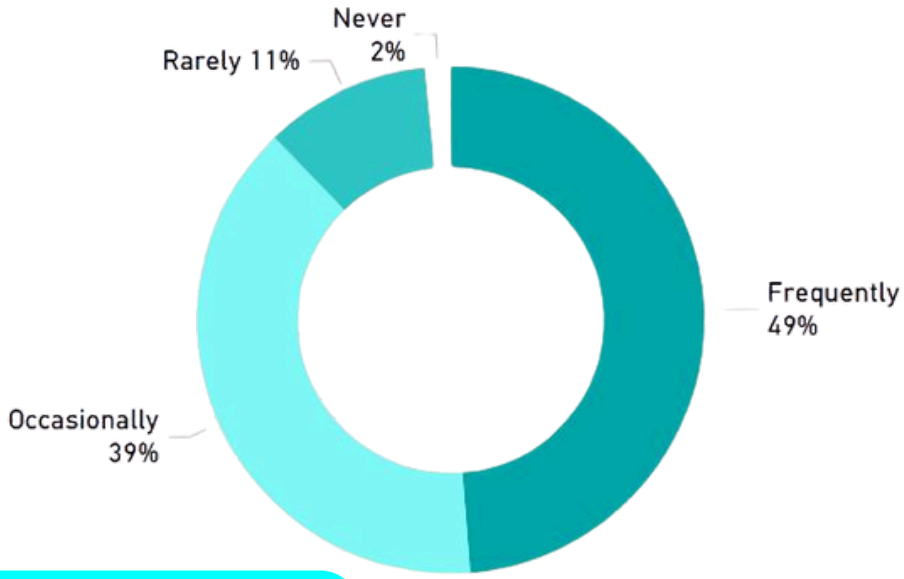
Functional independence and autonomy

Most respondents (66%) claim to have functional independence, however this aspect still proves to be a challenge for many DPOs whose autonomy is partially affected (24%) or do not have such independence (10%).



Reporting to senior leadership

The need to report data protection issues to senior leadership was significantly present (except for a few cases that never felt such a need - 9%).



3/4 of DPOs reported that they were promptly attended to by senior leadership, despite the 15% who reported facing difficulties in getting an appointment.

49% of DPOs have frequent formal meetings with senior leadership (e.g., committee meetings, periodic reports, etc.).

While only 13% indicate that they never or rarely hold these types of meetings.

Back to index

Structure and resources

Conflict of interest

The issue of conflicts of interest raises significant doubts for organizations, which indicates that the orientations provided by the ANPD in its guidance [5] are not sufficient to overcome this challenge for organizations.

In the present research, this aspect is evident in that 80% of the DPOs refrained from responding about the type of conflict that exists in the exercise of their activities.

Among the valid responses received, the main conflicting situations are:

- Decision-making about processing activities in the organization
- Pressure/lack of autonomy to omit risks or indicate compliance of activities
- Need for prior approvals by boards

International comparison [6]

The international scenario also reveals that DPOs are often involved in carrying out tasks that lead to a conflict of interest, which is interpreted by competent authorities as a matter that still requires further guidance, despite the materials already published on the subject.

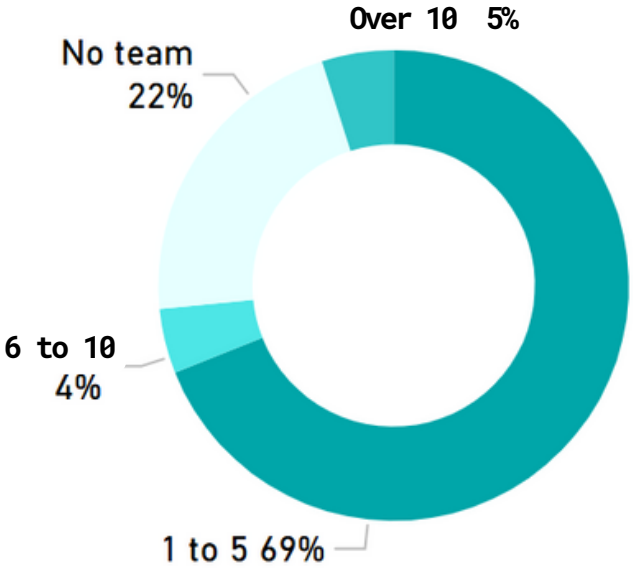
Back to index

[5] ANPD's guidance guide on the role of the person in charge (p. 34), available here.
[6] Designation and Position of Data Protection Officers, EDPB 2024 (p.3), available here.

Structure and resources

The organization must support the DPO in performing their tasks by providing the resources necessary to carry out these tasks, such as: human resources (such as a support team), available budget and tools.

Privacy Team



22% of DPOs responded that they work alone in their organizations.

Considering the cases of privacy teams, 69% of respondents stated that the team is made up of up to 5 people, and only 5% reported having a team with more than 10 people dedicated to privacy.

Furthermore, 55% of companies with more than 1,000 employees have privacy teams with 3 people or less.

International comparison [7]

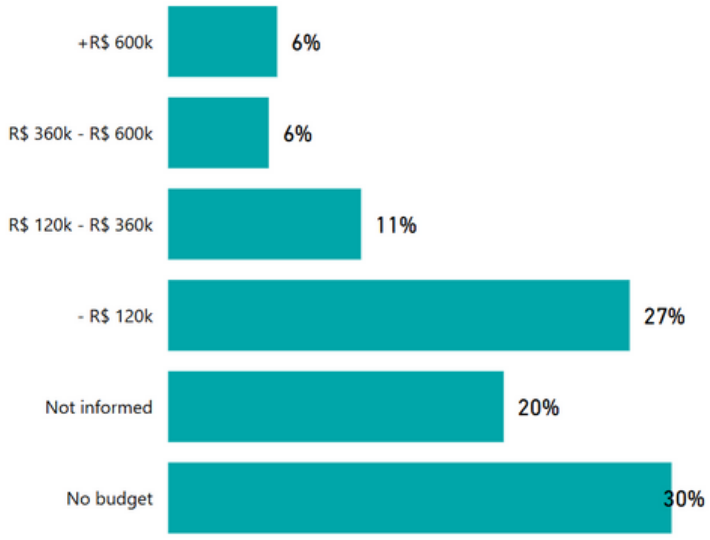
When analyzing the international scenario, there is a disparity in the size of teams dedicated to privacy, which vary according to region, with an average of approximately 29 employees in North American organizations, 26 employees in European companies, and 31 people in Asian companies.

Back to index

[7] IAPP Privacy Governance Report 2024 (p.29), available here.

Structure and resources

Annual budget allocated to privacy:

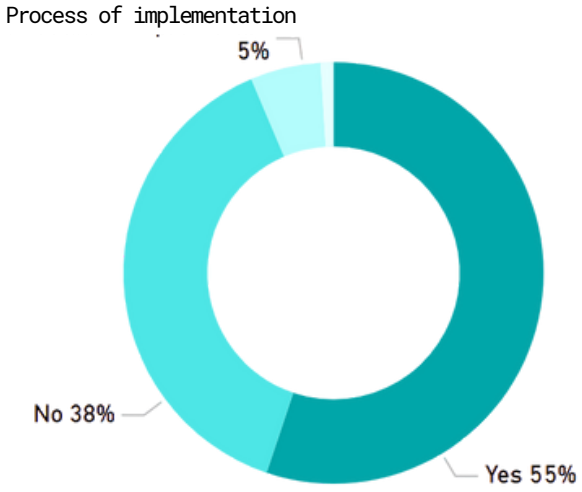


When asked "what is the budget allocated to privacy and data protection in your organization"—which excludes resources allocated to employee compensation—approximately 27% of respondents indicated that the annual budget is less than R$120,000. Twenty-four percent indicated a larger budget, potentially reaching or exceeding R$600,000 per year.

International comparison [8]

Despite growing awareness of the importance of data protection, the budget allocated to it remains suboptimal in Brazil. Survey data reveals that 74% of respondents from companies with more than 1,000 employees have less than R$600,000 per year allocated for this purpose. In comparison, global companies of the same size invest, on average, between US$1 million and US$7 million annually in data protection, highlighting the need and potential for greater investment in the sector.

Support tools:



The tools in use or in the process of being implemented by DPOs (60%) have the following modules as the most used:

- Record of Processing Activities (23%)
- Requests from Data Subjects (20%)
- Data Protection Impact Assessments/ Legitimate Interest Assessments (17%)
- Consent management (14%)
- Risk management (13%)
- Incident response (12%)

Back to index

[8] IAPP Privacy Governance Report 2024 (p. 25), available here.

Day-to-day

Provided for in art. 41 of the LGPD and regulated by Resolution CD/ANPD No. 18/2024, the DPO has functions such as:

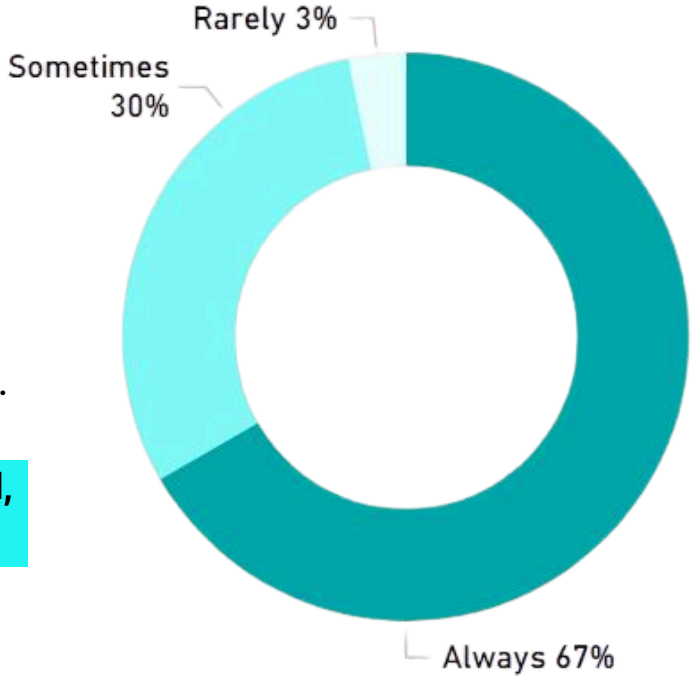
- Accept complaints and communications from data subjects and take action;
- Receive communications from ANPD; and
- Guide employees and contractors on personal data protection practices.

We asked the DPOs when they are involved in relevant data protection issues within the organization, as well as about the tasks that most occupy their day-to-day.

Involvement in decision-making

Although decision-making on processing activities is not a function of the Data Controller, they will often be involved or consulted to support such decisions within the organization - especially with regard to risk aspects and compliance with the LGPD.

67% of DPOs say they are always involved, while only 3% are rarely involved.



International comparison [9]

The data reveals a more positive scenario than that observed in the European Union, as only 21% of European DPOs claim to be always involved or consulted on data protection issues.

Back to index

[9] Designation and Position of Data Protection Officers, EDPB 2024 (p.22), available here.

Day-to-day

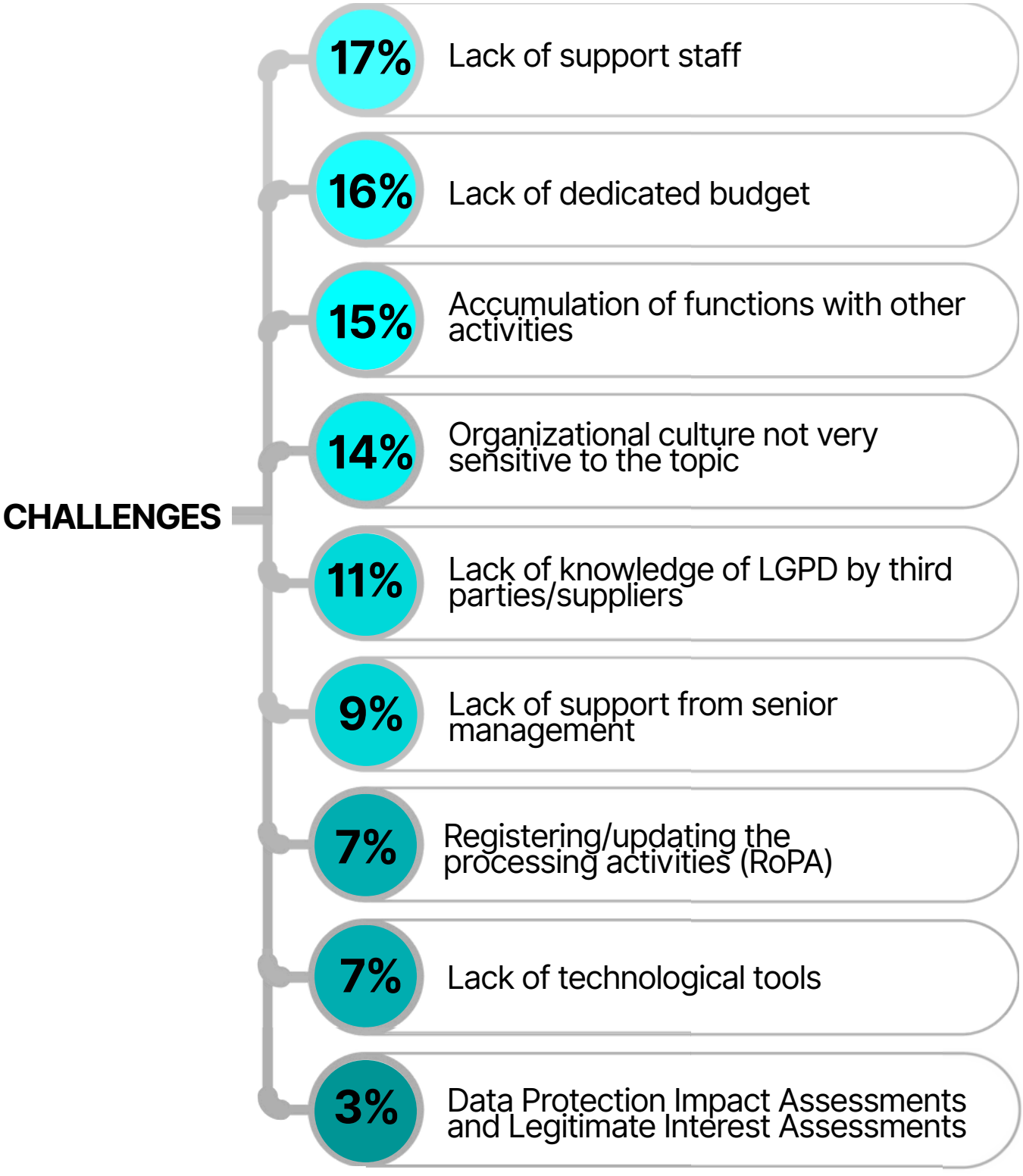
DPOs compiled their rankings based on the most frequent or time-consuming activities. The table below shows the choices that were most frequently ranked first, and which were most frequently placed on the podiums (1st, 2nd, and 3rd).

Position/ Activities	1st place	Top 3
Mapping/registering of processing activities	31%	49%
Response to various internal queries	17%	51%
Monitoring new projects (privacy by design)	15%	38%
Responding to data subject requests	11%	28%
Analysis, preparation or review of contracts	10%	35%
Structuring or reviewing internal policies, procedures and processes	8%	28%
Training and awareness actions	5%	22%
Data Protection Impact Assessments and Legitimate Interest Assessments	2%	27%
Management of external partners	1%	14%
Action in security incidents	0%	9%

Back to index

Day-to-day

DPOs presented the main challenges they face in carrying out their role:



Back to index

Day-to-day

Data breaches

Journey of identification and response to personal data breaches and stages in which the DPO indicates being involved:

Since initial identification **80%**

During the technical investigation **11%**

At this stage, it is common to confirm or deny the involvement of personal data.

After containment and technical analysis **7%**

Stage preceding any communication of the data breach to ANPD and data subjects

Not involved or there have been no incidents to date **3%**

International comparison [10]

The result obtained is consistent with the international scenario, specifically in the European context, given that 87% of DPOs claim to participate in the response to personal data breaches.

Back to index

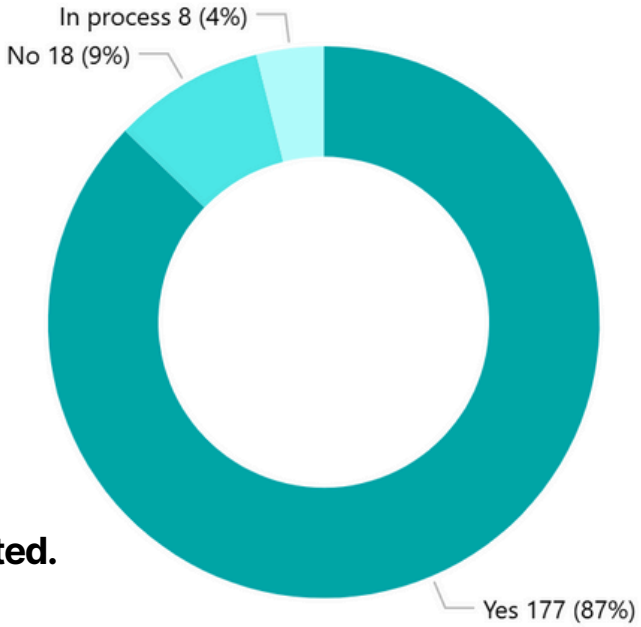
[10] Designation and Position of Data Protection Officers, EDPB 2024 (p.21), available here.

Governance

Defining a governance structure for managing the privacy program is the key to creating a culture of privacy. Furthermore, governance is closely linked to formal privacy policies and procedures.

Formalization of the position of DPO

The formal appointment of the DPO, whether internal or external, is established as a requirement under ANPD Resolution No. 18/2024. A formal act is understood as a written, dated, and signed document designating the position.[11]

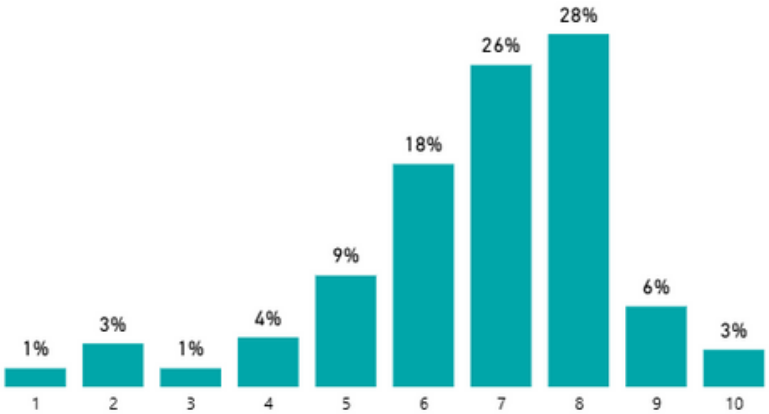


9 out of 10 **DPOs are appointed or in the process of being formally appointed.**

Maturity

An organization's level of maturity regarding privacy may be linked to perspectives on the mechanisms for managing LGPD requirements, such as the elements of the governance program provided for in Article 50 of this law.

Respondents were tasked with rating their perception of their organization's data protection maturity level from 1 to 10:



63% **assess maturity as high or very high**

of the organization on data protection (grades from 7 to 10).

Back to index

[11] The ANPD provides a model of a formal act for appointing the DPO, available as annexes to the Guidance for the DPO's performance.

Governance

Risk management [12]

The ANPD has published resolutions and materials regarding processing activities classified as high-risk due to their potential harm to data subjects. This classification is based on specific and objective criteria, which, when present together, lead to greater rigor in data protection, for example, through the preparation of a Data Protection Impact Assessment.[13]
Therefore, risk management of processing activities is an essential element for governance and monitoring of the DPO.

DPOs were asked about their risk perception regarding their organization's processing activities, indicating the level of risk on a scale of 1 to 10. By compiling the responses and classifying the risks as low (1-4), medium (5-6), high (7-8), and very high (9-10), we obtained the following results:

- **56% understand that high or very high risk activities are carried out**
- **16% understand that there are only low-risk activities**

Challenges encountered based on the perceptions of DPOs

Responses analyzing the risk of activities vs. the maturity of the organization

1/5 high or very high risk activities carried out in organizations with low or medium maturity (21%).

However, the highest rate of very high risk activities is present in organizations with high maturity (9%).

MATURITY \ RISK	Low	Medium	High	Very High
Low	3%	3%	2%	2%
Medium	3%	7%	11%	6%
High	9%	16%	20%	9%
Very High	1%	2%	4%	2%

Back to index

[12] art. 4 of Resolution CD/ANPD No. 2/2022, available here.
[13] Questions and Answers on the RIPD (question 9), published by the ANPD, available here.

Sectors

Key comparative and exemplary insights from the sectoral perspective:

Factors/ Sectors	**DPO Remuneration** over R$10k	**Budget for privacy** over R$360k	**Privacy Team** up to 5 people	**Hierarchical position of the DPO** as director or above
Health (20%)	48%	8%	68%	25%
Energy (8%)	75%	13%	69%	19%
Financial (12%)	79%	8%	75%	29%
Technology (19%)	76%	25%	68%	24%
Retail (9%)	61%	6%	78%	22%
Education (3%)	67%	17%	50%	33%
Others	77%	12%	71%	23%

Back to index

Conclusion

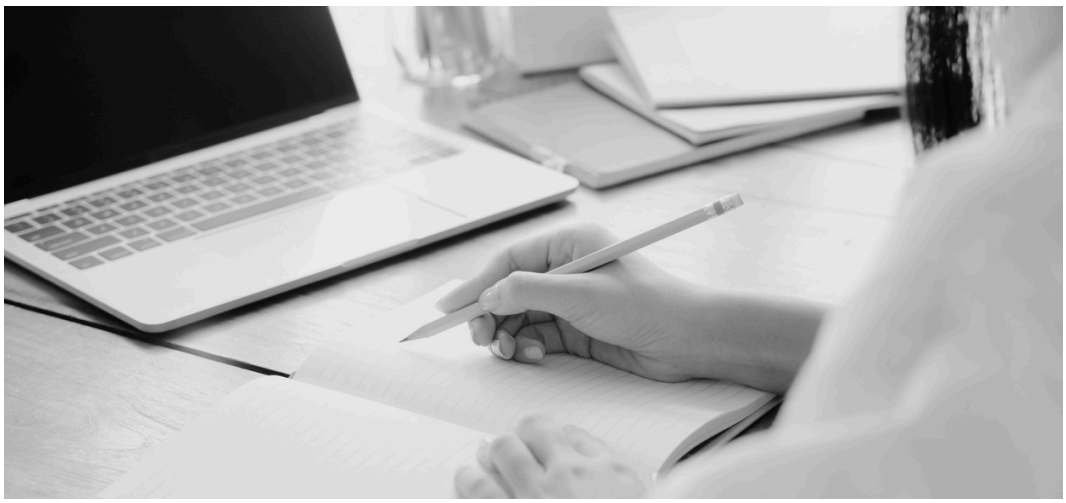
The research shows that the Data Protection Officer has gained more prominence in organizations, considering the positions taken and the frequency with which they are involved in discussions about privacy, in line with regulatory expectations for this role, which is essential for compliance with the LGPD.

When compared to the international scenario, especially with the European context that already has greater maturity in the topic of data protection, the DPO in Brazil presents a rapid evolution, considering the recent regulation of its activities in the country.

Without prejudice, there is still room for investment and improvement in this topic within organizations, directly impacting the performance of the DPO in the coming years.

Materials

Click on the links below and check out support materials on the topic of DPO in Brazil.



TO STAY UP TO DATE WITH THE REGULATORY SCENARIO:

CD/ANPD RESOLUTION No. 18, OF JULY 16, 2024
Approves the Regulation on the actions of the person responsible for processing personal data

ANPD's Guidance on the DPO's Performance (December 2024)

Opice Blum E-book on the role of the DPO

FOR TRAINING IN ACTIVITY AS DPO:

Check out the course offered by Opice Blum Academy:
Qualification for Data Protection Officer – DPO
contato@opiceblumacademy.com.br

About Rede Líderes

Ecosystem of people and businesses

Rede Líderes connects professionals from different fields who are experiencing the challenges of digital transformation firsthand. It supports leaders and organizations in expanding their relationship base, validating decisions, and discovering technological solutions based on those who already use and trust them.

Join us! **assessoria@redelideres.com**

About Opice Blum

Opice Blum Advogados is synonymous with digital innovation.

Since 1997, the law firm has partnered with its clients, redefining the limits of what's possible and bringing new strategies to meet new needs. With a team of expert lawyers, here is where transformation happens and stands out for its excellence in areas capable of positively impacting the sectors in which it operates, such as Data Protection, Information Security, Digital Litigation, and Legal Innovation, among others.

Visit **opiceblum.com.br**

Authors

Vitor Magnani
Founder of Rede Líderes
President of Movimento Inovação Digital

Henrique Fabretti Moraes
Partner and CEO of Opice Blum Advogados
Advisor and Legal Leader of Rede Líderes

Tiago Neves Furtado
Partner in Incident Response & Cybersecurity and Data Protection of Opice Blum Lawyers

Opice Blum Team

Editing and data analysis
Ana Rita Bibá Gomes de Almeida
Tatyana Patricia Lima Uchida
Helena Dominguez Paes Landim Bianchi
Lucas Mendes do Nascimento
Diego Carmona Pinange
Agla Myrella Coucolis

Research
Camila de Araújo Guimarães
Gabriela Silveira Bueno dos Santos
Artur Simões Campelo de Araújo
Cristiane de Souza Machado
Flavia Oliveira Gonçalves
Gabriela Alcântara da Silva
Jones Oliveira da Silva Junior
Manuella Filadoro Feiteiro Gonçalves
Marina de Paula Souza Reis
Patrícia de Oliveira Moraes Rossi
Rebeca Arima
Ricardo Nery Ramos


Opice
BLUM
Rede Líderes